TUTTO QUELLO CHE GLI ALTRI NON DICONO

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€

HACKER JOURNAL

n.176
www.hackerjournal.it

IL PROCESSO
PIRATE BAY
LA BAIA RESISTE



HACKING
SNORT
DIFENDIAMO LE RETI

MUSICA
IN ONDA CON LA NOSTRA
PIRATE RADIO

CRACKING
RAINBOW TABLES
ATTACCO ALLE PASSWORD

SECURITY
RINTRACCIAMO IL NOTEBOOK RUBATO

HARDWARE
HACKING I 100 VOLTI DI UNA STAMPANTE

QUATTORD. ANNO 9 - N° 176 - 14/27 MAGGIO 2009 - € 2,00
WLF PUBLISHING

Anno 9 – N.176
14/27 maggio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

HACKER JOURNAL

Si riparte...

"...a seguito dell'ingiunzione del pretore Grassi di Bologna che, attraverso l'Escopost, ha ordinato la disattivazione di tutti gli enti radio delle emittenti private..."
(Vasco Rossi, 1983)

Venerdì 17 aprile 2009, ore 11 del mattino, Peter Sunde, Fredrik Neij, Gottfrid Svartholm e Carl Lundström sono stati riconosciuti colpevoli da un tribunale svedese e condannati alla prigione e al pagamento di 2,7 milioni di euro di multa per 34 infrazioni alle normative sul copyright.

Una condanna non grave come è stata riportata dalla maggior parte dei media e dai comunicati stampa di esultanti Major (ma c'è differenza?). A causa della struttura della giustizia svedese, il tribunale che li ha giudicati non ha molto valore quando si trattano temi come la libertà individuale, il diritto internazionale, la costituzione. Prima di avere un responso realistico occorrerà almeno un altro grado di giudizio e i ragazzi della Baia lo sanno benissimo.

Infatti, The Pirate Bay è ancora lì, esattamente uguale a prima.

Con i suoi .torrent a disposizione di chiunque ne faccia richiesta e tutti i servizi connessi: SlopsBox, BayWords, BayImg, PasteBay e il nuovo IPREDator. Quest'ultimo non è altro che l'evoluzione naturale della pressione delle Major che, al grido (già sentito in tempi infelici) "colpirne uno per educarne cento", hanno deciso di inchiodare la Baia. IPREDator non è altro che una grande VPN creata su misura per la condivisione dei file: connessioni cifrate, non intercettabili, stabili. VPN che si aggiunge a quelle già diffuse con Hamachi e Wippien.

Una risposta in grande stile, in salsa social, che vede la partecipazione di altri protagonisti del download che forniscono strumenti dall'approccio alternativo, underground e dirompente. Un nome su tutti: OneSwarm. Si condivide qualsiasi cosa ma solo con gli amici, senza server centrale e senza alcun tipo di indice originario. Senza tracker. Perché i tracker non possiedono materiale protetto ma, vista la spinta di queste ormai vetuste potenze economiche internazionali, anche il semplice parlare di condivisione equivale a una condanna.

Quindi tanto vale passare al P2P di nuova generazione. Proprio per questo, passata l'iniziale delusione, una analisi della condanna svedese si traduce in un vero trionfo della libertà, confermato dai numeri: il partito pirata svedese ha indici di crescita a due cifre e probabilmente avrà almeno un seggio alle prossime elezioni europee, il materiale disponibile sui circuiti P2P è decuplicato, il boicottaggio delle Major sta facendo crollare le vendite di CD e DVD, gli utenti stanno passando in massa a più evoluti sistemi di condivisione.

La condanna di Davide, per altro inutile, sta dando il colpo di grazia a Golia.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Social sotto attacco

Kaspersky Lab ha annunciato di aver individuato un virus di tipo worm capace di interferire con il corretto funzionamento di Twitter: è il primo virus esplicitamente rivolto agli utenti dei social network. Alla base del funzionamento di questo virus, diffuso l'11 aprile e chiamato Net-Worm.JS.Twettir, c'è una vulnerabilità, ora corretta, del sito di Twitter: la possibilità di eseguire codice cross site (XSS) per modificare un account. Non appena si visita un profilo infetto, si viene contagiati. La rapida diffusione di questo worm è stata causata dal fatto che nessuno si aspettava un attacco del genere e anche se i creatori di Twitter sono corsi immediatamente ai ripari, il numero di contagi iniziali ha fatto presagire il peggio. Fortunatamente, grazie alla correzione dei problemi del noto social network e a tempestivi aggiornamenti degli antivirus, l'infezione non è poi stata in grado di espandersi ulteriormente. Come spesso accade, però, occorre notare che alla prima ondata se ne sono succedute altre, causate da varianti del virus originale. Virus che, per altro, è risultato facilmente modificabile a causa del massiccio utilizzo di codice JavaScript. Responsabile iniziale di tutta l'operazione sembra essere stato un ragazzo di 17 anni che, in una intervista alla rete televisiva NBO, ha ammesso di aver creato il virus per noia e per promuovere il proprio sito attraverso i messaggi del worm. Pur non avendo a che fare con un virus particolarmente sofisticato, questa rivelazione fa certamente riflettere, visto che sono in crescita episodi di bullismo telematico: atti dannosi per un intero sistema sociale, pur virtuale, compiuti più per noia e stupidità che per necessità. L'unico suo merito, allo stato attuale, non riguarda l'informatica ma la sociologia: aver attirato l'attenzione sul fatto che l'abitudine degli utenti di social network di visitare qualsiasi profilo e l'invito delle società di gestione a farlo, in alcune situazioni e con gli utenti meno smaliziati, sono indistinguibili dai messaggi tipici di un virus che ha infettato un sistema. Un campo che si apre prepotentemente, quindi, proprio nel momento di maggior espansione dei siti di social network e che costringe utenti, gestori e osservatori a riflessioni che vanno al di là delle considerazioni tecniche.



IL GPS ORA DIVENTA ECOLOGICO

Il navigatore satellitare riduce i consumi di carburante perché aiuta gli automobilisti a non perdersi, a scegliere i percorsi più brevi e ad evitare il traffico. Questo è il risultato di un'indagine del produttore Navteq che ha monitorato un gruppo di automobilisti nelle aree di Dusseldorf e Monaco di Baviera. Dai test è emerso che i consumi di chi ha un GPS in auto diminuiscono di circa il 12% per ogni 100 Km per un risparmio annuale stimato in circa 400 euro. Il merito è da cercare nulle nuove tecnologie di map sharing e traffic control, che permettono di sapere in tempo reale quali sono le strade meno battute e segnalano la presenza di lavori sul percorso consigliando eventuali deviazioni.

NAVTEQ ON BOARD

BUCATO IL FIRMWARE 3.0 DELL'IPHONE

Nel mese di marzo Apple ha presentato la nuova versione del firmware per il suo iPhone che introduce numerose novità come la gestione degli MMS, il tethering (ovvero la possibilità di utilizzare il telefono come modem per collegarlo al PC) e un programma per tagliare e montare i filmati. Questo nuovo software sarà disponibile sia per gli attuali iPhone 3G che per il prossimo smartphone che verrà presentato a giugno. La notizia però è che gli hacker del DevTeam (che già avevano ripetutamente sbloccato il telefonino della Mela) hanno bucato anche il nuovo software, per il momento rilasciato in versione beta ai soli sviluppatori. La chiave per effettuare l'hacking è stata la presenza di un bug di programmazione che ha aperto la porta ai pirati, increduli per il regalo di Apple. Insomma, il nuovo iPhone deve ancora nascere e già è disponibile il software per sbloccarlo e permettere l'installazione di applicazioni non originali. Che dire, craccare in anticipo un software prima che venga rilasciato non è da tutti. Apple ne sarà sicuramente contenta.



L'UE CONTRO SARKOZY NELLA LOTTA ALLA PIRATERIA

Giustizia è fatta! Finalmente l'UE ha capito che il giro di vite contro la pirateria informatica e il download di file, musica e video dal Web non poteva coinvolgere in modo così diretto i provider. Per intenderci, il premier francese Sarkozy aveva caldeggiato la proposta di legge (poi ribattezzata proprio "dottrina Sarkozy") che costringeva i provider a denunciare i propri utenti nel caso rilevassero un uso non consentito della loro connessione al Web. La proposta aveva fatto insorgere numerose associazioni di consumatori, ma anche i provider che avrebbero incontrato difficoltà tecniche, oltre che etiche, per monitorare così attentamente l'utilizzo della loro rete. Per fortuna l'Unione Europea si è espressa sulla questione ribadendo che la lotta alla pirateria è di competenza delle autorità e che i provider devono mantenere solo un atteggiamento di piena collaborazione (per altro già presente) nel caso un magistrato richiedesse loro informazioni su particolari utenti. La denuncia preventiva quindi resta un atto di terrorismo, che però la Francia conosce bene: dopo la (giusta) Rivoluzione Francese infatti, per essere condannati a morte come filomonarchici, bastava una denuncia, anche infondata e anonima...

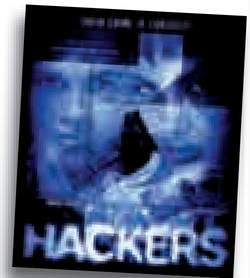




HOT NEWS

STATI UNITI COLABRODO

RUBATO UN ALTRO PROGETTO SEGRETO



È di qualche giorno fa la notizia data dal Wall Street Journal che alcuni hacker sono riusciti a violare il complesso sistema di sicurezza informatico del Pentagono impadronendosi dei piani segreti per la costruzione di un super bombardiere americano. Pare che gli abili pirati sono riusciti a scaricare decine di Terabyte (quindi non solo qualche disegno) di dati relativi al nuovo progetto miliare statunitense, compresi i sistemi di sicurezza, innesco e lancio delle bombe. Insomma, un furto in piena regola. Questo attacco non è certo il primo e non sarà l'ultimo, ma preoccupa il fatto che il sistema di difesa informatica del Pentagono abbia subito decine di violazioni dall'inizio dell'anno: voci non confermate ma provenienti dalla CIA indicano la Cina come principale fonte degli attacchi.

IL VIRUS RAPITORE CHIEDE IL RISCATTO

Sembra un racconto di fantascienza, invece e la realtà. Si tratta di un nuovo virus sviluppato da astuti pirati informatici in grado di criptare un intero hard disk in pochi minuti. Krypt.cz è un software di codifica dati che, dopo aver reso illeggibili i dati del PC infettato, mostra il seguente messaggio: "Tutti i vostri archivi sono cifrati". Se desiderate decodificarli, dovete comprare il decodificatore, che costa 900 euro. Come comprarlo? Potete inviare i soldi via Western Union o con il trasferimento bancario. Selezionate il metodo preferito e vi invieremo i dettagli per il pagamento. Dopo averlo effettuato, mandate una email all'indirizzo buyadnfly@ gmail. com, con la ricevuta e il file crypt.txt. Quando riceveremo i soldi, vi invieremo un decodificatore. Non provate a minacciarci o a offenderci, perché non accetteremo più i vostri soldi e smetteremo di rispondere alle vostre email. Voi così perderete per sempre i vostri archivi e i vostri documenti importanti". Accettando le condizioni, riceveremo un file con il codice per decriptare nuovamente l'hard disk. Il virus, intercettato sul PC di un utente di Sassari, è noto alle autorità che qualche anno fa neutralizzarono la sua prima versione.



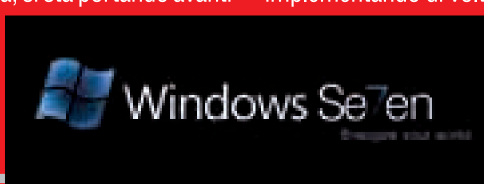
OPEN HACK DAY BY YAHOO

Nella cornice del Congress Centre di Great Russel Street si terrà il 9 e 10 maggio l'Open Hack Day, una manifestazione organizzata da Yahoo per incontrare i migliori sviluppatori indipendenti della scena mondiale. L'evento, che vedrà oltre 200 partecipanti tra programmatori e fan dell'hacking, ha come obiettivo quello di sviluppare nuove applicazioni per le piattaforme software di Yahoo denominate "open strategy". La manifestazione prenderà il via il 9 maggio alle 8,30 per poi entrare nel vivo con la 24 ore vera e propria che si concluderà il giorno 10 alle ore 13,30. Si tratta di un'opportunità molto importante sia per gli sviluppatori di Yahoo che potranno confrontarsi con le migliori comunità di hacker del pianeta, sia per i programmatori indipendenti che avranno una vetrina per mettersi in luce. Per non parlare degli appassionati di hacking, che potranno vedere tanti talenti tutti insieme: sarà proprio uno spettacolo interessante.



Windows: il 7 e l'8

La Release Candidate è arrivata da qualche giorno sui PC dei tester di Microsoft e entro la fine dell'anno dovremmo vedere il nuovo sistema operativo sugli scaffali dei negozi. Eppure Microsoft sta già lavorando a Windows 8! L'azienda di Redmond non si ferma e, dopo aver tirato fuori il suo nuovo sistema operativo in meno di 2 anni dall'uscita di Vista, si sta portando avanti anche su quello del futuro, che dovrebbe vedere la luce alla fine del 2011. Dopo aver tenuto l'ottimo XP sul mercato per oltre 7 anni, Microsoft si è accorta che vendere un sistema operativo ogni 2 anni potrebbe essere un buon modo per fare cassa e quindi sta già pensando a come spennare i suoi clienti per i prossimi anni. La notizia è più di una semplice voce, visto che è stata pubblicata direttamente sul blog ufficiale di Microsoft. Invece di creare un sistema operativo stabile e aggiornabile, Microsoft si perde implementando di volta in volta funzionalità inutili che aumentano il prezzo del prodotto come quegli "Ultimate Extras" promessi e mai sviluppati, per la gioia di coloro che si erano comprati la versione Ultimate in attesa di aggiornamenti.



IL COPYRIGHT? DURA 70 ANNI

Si allunga la durata della validità dei diritti d'autore, ovvero periodo di tempo in cui occorre pagare dei soldi per godersi una canzone o un film. Il Parlamento Europeo ha infatti deciso di prorogare il diritto d'autore dai 50 previsti fino ad oggi fino a 70 anni. Una legge che sicuramente fa discutere e favorisce le Major che detengono i diritti discografici e i discendenti di famosi artisti che sarebbero costretti ad andare a lavorare davvero invece di godersi i proventi dei loro illustri parenti. In realtà il danno maggiore è per i consumatori, che oggi avevano la possibilità di scaricare gratuitamente, riprodurre e utilizzare senza pagare alcunché brani che hanno fatto la storia della musica, come i primi album dei Beatles, di Elvis e di tanti altri grandi artisti. Nulla di fatto, dovranno aspettare altri 20 anni grazie a tale parlamentare McCrevy, scagnozzo delle industrie discografiche e cinematografiche che addirittura aveva proposto una proroga a 95 anni. C'è da dire, per completezza, che una parte dell'estensione dei diritti sarebbe andata a quei musicisti, ormai pensionati, che hanno contribuito a rendere grande la musica degli anni '50: loro se li sarebbero meritati, ma avrebbero ricevuto solo l'1% di quanto incassato dalle Major.



UN NOKIA CHE VALE ORO... PER I PIRATI

Qualche mese fa, su eBay un anonimo utente ha acquistato un vecchio cellulare Nokia 1100 per l'incredibile somma di 25.000 euro. Potreste pensare ad un errore o ad un autentico "pollo", ma la realtà supera l'immaginazione. L'acquirente non è altro che uno dei tanti kracker, ovvero criminali informatici, che hanno scoperto una vulnerabilità davvero interessante nel software di questo telefono. Pare infatti che il Nokia 1100 presenti un piccolo bug di programmazione che permetterebbe ai pirati di intercettare le password di accesso inviate dalle banche via SMS per accedere ai conti online. In pratica, ormai molte banche utilizzano un sistema di password temporanee da abbinare a quella in nostro possesso, per autorizzare l'accesso al conto online: il Nokia 1100 appositamente modificato permetterebbe di clonare ogni tipo di SIM e ricevere questi dati al posto del destinatario. Con un po' di abilità e l'hacking contemporaneo del PC del malcapitato sarebbe quindi possibile rubare i dati di accesso e di ripulire il suo conto corrente. La notizia non è stata ancora confermata e anche Nokia stessa cade dalle nuvole: intanto su eBay si moltiplicano le offerte per i 1100 venduti a cifre astronomiche. Che dire, se ne avete uno, vendetelo!





LASER: LA NUOVA FRONTIERA KEYLOGGING

Keylogger sono dei particolari software che registrano le sequenze di tasti che digitiamo sulla tastiera e vengono utilizzati principalmente dai criminali informatici per rubare password e codici di carte di credito. In realtà, per ottenere un risultato simile e molto più discreto non serve installare un programma sul PC, ma basta un microfono laser e un software in grado di interpretare la registrazione. La trovata è di una coppia di hacker italiani che hanno scoperto come, grazie a un particolare strumento laser oscilloscopico del costo di 60 euro, sia possibile rubare i dati di un PC senza interagire con il computer e a una distanza di decine di metri dal dispositivo. Orientando il microfono laser verso la finestra della camera in cui si trova il PC, questo sarà in grado di registrare tutti i rumori (anche quelli a bassa frequenza) prodotti dalla tastiera del PC. Non serve altro che un software sviluppato dai due programmatori per convertire i clic della tastiera nel tasto corrispondente: questo è possibile grazie alla sensibilità del microfono, che riesce a mappare le impercettibili variazioni sonore date dalla diversa inclinazione delle dita sui tasti. Il programma è anche in grado di imparare e capire velocemente lo stile di ogni utente via via che i segnali vengono elaborati.





HOT NEWS

TELEFONARE IN AEREO... CON RYANAIR SI PUÒ

Da poche settimane è partita la sperimentazione da parte del vettore low cost Ryanair per permettere ai propri passeggeri di utilizzare il telefonino per chiamate e messaggi anche ad alta quota.



Per il momento il servizio è attivo solo su pochi velivoli che partono da Roma Ciampino, ma Ryanair assicura di poter estendere la possibilità di utilizzare il cellulare in volo a tutti i suoi aerei entro il 2010. Se volete togliervi lo sfizio di chiamare casa dall'aereo però, sappiate che le tariffe sono tutt'altro che economiche: il roaming internazionale, unito al costo aggiuntivo del servizio, porta il costo di un minuto di conversazione a 2-3 euro. I messaggi invece costeranno 50 centesimi ed è possibile telefonare con tutte le compagnie italiane, Tim, Vodafone, Wind e 3. Una sola riflessione: visto che Ryanair effettua brevi tratte (massimo 2 o 3 ore di volo), è proprio indispensabile avere il telefonino acceso anche durante il viaggio?

PER LA LOPEZ SICUREZZA MADE IN ITALY

L'immagine di un'artista è qualcosa di molto prezioso e difficile da proteggere. Soprattutto online, dove può circolare ogni tipo di immagine o notizia in grado di danneggiarla pesantemente. Per questo la popolare cantante e attrice latina Jennifer Lopez ha deciso di ingaggiare un professionista per monitorare e gestire la sua immagine e proteggere le informazioni contenute nei computer delle sue ville dall'attacco di pirati informatici. La scelta dell'ex compagna di Ben Affleck è ricaduta su un esperto italiano, Fabio Ghioni, capo del team di Tavaroli nella vicenda tristemente nota delle intercettazioni telefoniche Telecom. Ghioni è comunque un vero esperto del settore e utilizzerà ogni tipo di apparecchiatura a sua disposizione per mettere in sicurezza il patrimonio informatico della Lopez. Gli attori hollywoodiani avevano già scelto l'Italia come residenza per le vacanze, per la moda e il cibo: si vede che anche nell'informatica stiamo raggiungendo gli stessi livelli di eccellenza.



2009, L'ANNO DEI VERMI

I laboratori di F-Secure hanno lanciato un preoccupante allarme dopo aver monitorato le minacce sul web per i primi 3 mesi del 2009: attenti ai Worm. Sono virus in grado di infettare il sistema, replicarsi e rubare informazioni preziose o, in alternativa, prosciugare le risorse del PC rendendolo inutilizzabile. F-Secure ha notato come questo genere di virus sia cresciuto esponenzialmente nei primi mesi dell'anno, generando mostri come Conflicker o SexView, primo worm dedicato agli smartphone. F-Secure ha anche rilevato i primi worm inseriti nelle applicazioni di Facebook, che possono infettare milioni di computer in poche ore. Il consiglio è sempre lo stesso: molta attenzione e un buon antivirus.



XBOX 360 PIÙ GARANTITA

Se diciamo "Errore E47" di Xbox360, vi viene in mente qualcosa? No? Allora siete tra i fortunati possessori della console Microsoft che non hanno visto apparire sullo schermo questo messaggio di morte all'accensione del dispositivo. L'errore E47, è una vera e propria condanna a morte per l'Xbox 360 visto che dovremo riconsegnare la console all'assistenza per la sostituzione. Fino a qualche tempo fa però questo errore non era contemplato tra quelli in garanzia e l'effetto della schermata nera era di fatto quello di farci buttare la console nel secchio della spazzatura. Peccato che in pochi mesi le console difettate sono aumentate esponenzialmente raggiungendo circa il 10% degli utenti: mica male! Per questo Microsoft ha deciso di fare un passo indietro e di includere l'errore E47 tra quelli coperti da garanzia. Non si tratta del primo difetto dell'Xbox 360 che già qualche hanno fa è stata bersaglio di critiche per una serie di malfunzionamenti dovuti alla ventola di raffreddamento che hanno messo KO circa un terzo dei dispositivi venduti. Si spera che questo sia l'ultimo difetto di una console che, pur essendo valida e accompagnata da un buon servizio online, non ha mai convinto gli appassionati di videogames.





Colpiti e affondati?

Baia condannata, la Baia chiude, la Baia è finita. Tutto falso. La Baia c'è ancora e non è mai stata così forte come ora

Una banale sentenza di primo grado di un processo in Svezia può essere trasformato in un evento mediatico di rilevanza mondiale? Può finire su tutti i giornali, su tutti i TG? Una sentenza di primo grado può essere una notizia per cui valga la pena tardare l'uscita in edicola? Se il processo riguarda i fondatori di The Pirate Bay, il più noto tracker di file Torrent del mondo, se la pubblicità al processo viene spinta dalle grandi corporation del globo, se in ballo non c'è la semplice condivisione di materiale protetto ma c'è una sfida tra diritti individuali ed economici, l'eco di una sentenza ha come minimo una rilevanza mondiale. Quello a cui abbiamo assistito in Svezia ha avuto scarsa importanza pratica, visto che si tratta di una sentenza di primo grado e non di una condanna definitiva, ma una rilevanza mediatica, politica, sociale enorme. I fondatori sono stati condannati alla prigione e a un'ammenda stratosferica non perché abbiano scambiato materiale protetto, ma perché gestiscono un sito che tiene traccia di questo materiale insieme ad altro di libero utilizzo. Non hanno scaricato nulla, non l'hanno messo in condivisione, non hanno infranto leggi: sono colpevoli di aver favorito lo scambio di materiale illegale. Nella realtà hanno solo creato uno strumento che, in nome della neutralità della Rete, dovrebbe essere considerato come tale. Per questo motivo la sentenza svedese ha un impatto sociale enorme: è un precedente di immensa importanza perché se venisse confermata nei gradi di giudizio successivi, qualsiasi programmatore potrebbe essere responsabile di come vengono utilizzati i suoi strumenti. Il che significa, sostanzialmente, dover rinunciare a tutti gli strumenti di tutela della privacy: client TOR, programmi di crittografia, remailer anonimi e così via. Qualcuno potrebbe usarli per preparare attentati o compiere azioni illegali, il che trasformerebbe i malcapitati programmatori in complici. Allo stesso tempo e per gli stessi motivi potremmo salutare le chat ma anche avere qualcosa da ridire a Google che indicizza pagine su come si costruiscono le bombe, dandoci la possibilità di trovarle e scaricarle.

:: Meglio non iniziare

Al di là delle previsioni più o meno catastrofiche per il futuro c'è da dare adito a questi ragazzi di restare fermi nelle loro posizioni: tutt'ora, nelle pagine del blog comune di The Pirate Bay campeggia una scritta emblematica: "The only winning move is not to play". È la scritta con cui il supercomputer di Wargames (film del 1983)



Dove vuoi trovare le dichiarazioni dello staff di The Pirate bay? Ovviamente in un file nei circuiti P2P, il cui torrent si può scaricare dal sito…

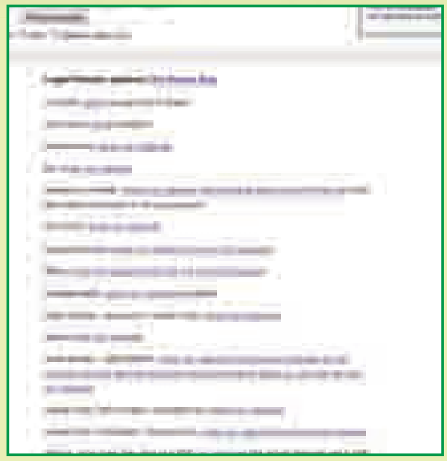
pone fine alla sua guerra atomica non tanto simulata. Messa su quelle pagine in tempi non sospetti, è una frase emblematica della situazione in cui si trovava The Pirate Bay. Da una parte le major che avrebbero voluto spazzarlo via quanto prima e dall'altra una comunità mondiale di singoli individui, pensatori, hacker, filosofi, artisti, gente comune, lo sosteneva direttamente o indirettamente, pensando che l'attuale tutela sul diritto d'autore (concepita nel '700) mal si adatta ad un mondo fatto di rapidissime contaminazioni come l'attuale. L'intento provocatorio di The Pirate Bay è stato chiaro fin da subito a chiunque si fosse preso la briga di leggere i testi presenti sul loro sito ma le major non hanno raccolto il confronto. Come le più tradizionali corporation dei romanzi cyberpunk hanno preferito lo scontro diretto, andando a colpire dove, per altro, non gli è nemmeno consentito garantirsi protezione immediata. Il sito è tutt'ora attivo e ci vorranno anni perché chiuda. Come il caso Napster insegna, la scomparsa di un soggetto non significa l'abbandono della tecnologia ma la sua evoluzione forzata verso qualcosa di diverso. Già oggi disponiamo di VPN, reti tra amici, reti distribuite di scambio e costringere alla chiusura The Pirate Bay significherebbe solo frammentare gli utenti dirigendoli verso sistemi più evoluti e, per ora, a prova di intercettazione. D'altra parte alla Baia lo sapevano bene cosa avrebbe comportato uno scontro legale. Tecnicamente non condividono materiale protetto e hanno, anzi, dimostrato come gran parte del materiale indicizzato dal sito sia di libero utilizzo. In più sono accusati di complicità in un reato per cui i colpevoli sono distribuiti sull'intero pianeta e sono, purtroppo per le major, moltissime persone. Proprio questo aspetto è quello più devastante nell'immediato: il Partito Pirata svedese non ha mai visto tante adesioni, le vendite di prodotti delle major sono in crollo a causa del boicottaggio iniziato dai sostenitori della Baia e diffuso a macchia d'olio grazie ai social network, la pubblicità gratuita per The Pirate Bay è stata enorme. Un insieme di cose che fa della condanna in primo grado una vittoria di Pirro per tutte quelle società che faticano a comprendere che il loro business è cambiato.

:: Dategli brioches!

Proprio questo è il nocciolo della questione, quella che va oltre il semplice scambio di file, quella per cui l'affaire The Pirate Bay rappresenta solo una scaramuccia iniziale. Con la struttura attuale della società, con i mezzi tecnici di cui si dispone, con comunicazioni che prevedono scambi immediati con il resto del mondo, con la diffusione sempre più elevata di una mentalità "open", il mercato tradizionale è



Un sito spoglio: la stessa filosofia di Google… Che sia condannabile anche questo? Dopotutto indicizza cose proibite ben peggiori di qualche file illegale.



Nella sezione legale di TPB sono riportate mail ricevute e risposte date… basta una lettura veloce per rendersi conto della provocazione cercata e ottenuta.

destinato a cambiare o a sparire. I timidi tentativi delle major di trasformarlo a loro uso e consumo si sono arenati in aride discussioni su lucchetti DRM e protezioni anticopia che hanno solo danneggiato i loro acquirenti legittimi e tradizionali, favorendo un'ulteriore conversione a un mercato più aperto. La nascita di concorrenti capaci di sfruttare questo nuovo mercato con un modello di business adeguato e profittevole le ha messe ulteriormente in crisi. Gli artisti che hanno avuto maggiore sensibilità hanno iniziato a condannarle. Ora la nuova tegola: la vittoria al processo alla Baia. Un gesto che è paragonabile alla risposta della leggenda che vuole far rispondere a Maria Antonietta "Allora dategli brioches!" al popolo che si lamentava della mancanza di pane. Il margine per trasformarsi e adeguarsi alla mentalità della folla è stretto, i movimenti sociali planetari stanno decidendo autonomamente, la recessione economica non fa altro che peggiorare le cose mentre i movimenti "open" non ne vengono toccati. Le Major lo sanno bene e dovranno stare attente: se non si trasformeranno in modo radicale, la gente farà ben presto a meno di loro e sarà difficile ricorrere ai tribunali per costringere le persone a fare acquisti. E la Baia? Staremo a vedere: i ragazzi sono sicuri del fatto loro e hanno fiducia nella bontà e giustizia della legge svedese. E noi con loro.



È rivoluzione: liberalizzato l'archivio di indirizzi del sito iplocationtools.com

IP fa rima con SQL

In un periodo di minacce informatiche assortite, fa piacere che la Rete ci riserva qualche gradevole novità. Una delle più sfiziose ai fini hacker è quella che coinvolge il mitico sito iplocationtools.com. Benché non abbia bisogno di molte presentazioni, per chi non lo sapesse di tratta di un servizio online che consente di "geolocalizzare" un indirizzo IP. Quindi, in pratica, basta dargli un qualsiasi indirizzo IP e lui ne visualizza la provenienza su una mappa. Magari può sembrare una caratteristica scontata, del resto i siti che offrono questo servizio non mancano, ma in realtà è la sua tecnologia a presentare numerosi spunti di riflessione.
Si basa, infatti, sulla consultazione ottimizzata di un vasto database SQL, organizzato in modo da fornire i risul-



In aggiunta alla consultazione, finalmente il database è disponibile in download sia in formato SQL che CSV.



Ovviamente ci rimane la possibilità di utilizzare l'archivio direttamente dal sito Web, andando nella sezione IP Lookup.

[Codice 1]

```
ip = ((A*256+B)*256+C)*256
```

(assumendo che D, cioè l'ultima parte dell'indirizzo, sia 255)

tati con ridottissimi tempi di risposta. Il database rappresenta giocoforza il cuore del sistema, ed è aggiornato con elevata frequenza. Anche perché i gestori del sito offrono servizi di consulenza, e dunque lo coccolano come loro fiore all'occhiello. La notizia eclatante è che questo gioiello SQL, dallo scorso aprile, è stato "liberalizzato".

Proprio così: chiunque può scaricarlo dal sito ufficiale iplocationtools.com, sia in formato SQL sia CSV. Per la maggior parte degli utenti, ovviamente, la prima versione è quella più interessante, perché può essere comodamente inserita nel proprio server al fine di creare un servizio simile a quello originario (di iplocationtools.com). Non di meno, visto che i file SQL sono in formato di testo in chiaro, possono essere consultati con le tradizionali funzioni di ricerca. Tuttavia, questo favoloso database ha le sue precise regole di consultazione, che vale la pena approfondire.

:: Scarichiamo il database

Per prima cosa, dunque, dobbiamo scaricare l'archivio. Andiamo su www.iplocationtools.com/sql_database.php, poi clicchiamo, a scelta, su SQL format Download link o su CSV format Download link (nel nostro esempio selezioniamo il formato SQL). Il primo file, ipinfodb.sql.bz2, è nel formato compresso BZ2, ben supportato dal software gratuito ZipGenius (www.zipgenius.it). una volta aperto l'archivio, estraiamo il file ipinfodb.sql in una cartella a piacere (va bene anche il desktop di Windows). Di fatto, questo archivio ora può essere utilizzato come un qualsiasi file SQL.

[Codice 2]

```
SELECT * FROM `ip_group_city`
```

(dove l'indirizzo IP di partenza deve essere inferiore o uguale al valore ottenuto dalla formula)

Tuttavia, è bene spendere qualche parola sulla sua struttura. Prima di tutto, gli indirizzi IP contenuti al suo interno sono elencati nella tabella ip_group_city, e NON nel classico formato IPv4 A.B.C.D (es. 192.192.168.168). Questo per evitare problemi di accesso ai dati. Viene invece utilizzata una formula del tipo descritto in **Codice 1**.

A questo punto, la ricerca all'interno del database SQL può essere effettuata con l'istruzione di **Codice 2**.

Queste semplici istruzioni sono sufficienti per gestire i dati dell'archivio, con un'efficienza elevatissima. Il merito della velocità di ricerca sta nel basso numero di campi, che si aggira sugli 1,4 milioni. Notevole, se pensiamo che l'equivalente di un concorrente come Geolite City ne vanta oltre 3 milioni. A questo punto, sorge il dubbio: non è che con "soli" 1,4 milioni di indirizzi rischiamo di fare ben poco? Di effettuare ricerche troppo approssimative? In realtà, come anticipato, il databse di iplocationtools.com funziona sulla base di un'elevata ottimizzazione. Semplificando, si basa non su singoli indirizzi IP ma su "blocchi", registrati uno per riga.

:: Facile da programmare

Chiarita la struttura e l'accessibilità di questo favoloso database, arriviamo al suo utilizzo programmativo, per chi di noi desideri mettervi mano. Dunque, se vogliamo memorizzarlo e usarlo nel nostro server, ecco un esempio di funzione PHP pronta all'uso, per effettuare le ricerche, **Codice 3**.

[Codice 3]

```
function locateIp($ip){
  $d = file_get_contents("http://www.iplocationtools.com/ip_query.
_php?ip=$ip&output=xml");
if (!$d)
  return false; // Failed to open connection
  $answer = new SimpleXMLElement($d);
  if ($answer->Status != 'OK')
  return false; // Invalid status code
  $country_code = $answer->CountryCode;
  $country_name = $answer->CountryName;
  $region_name = $answer->RegionName;
   $city = $answer->City;
  $zippostalcode = $answer->ZipPostalCode;
  $latitude = $answer->Latitude;
  $longitude = $answer->Longitude; //Return the data as an array
  return array('latitude' => $latitude, 'longitude' => $longitude, 'zippostalcode' =>
_$zippostalcode, 'city' => $city, 'region_name' => $region_name, 'country_name' =>
_$country_name, 'country_code' => $country_code, 'ip' => $ip);
}
```

Una volta implementata la funzione, all'occorrenza è sufficiente richiamarla con il comando:
http://iplocationtools.com/ip_query.php?ip=xxx.xxx.xxx.xxx.

Per ottenere il responso desiderato.



Facciamo sentire la nostra voce in rete

PIRATE RADIO

Chi fra noi conosce la frase "Credo nelle rovesciate di Bonimba, e nei riff di Keith Richards" detta da Freccia nel mitico film di Luciano Ligabue, di sicuro non farà fatica a immaginare la sensazione che si può provare a parlare in radio, lanciando nell'etere un messaggio che può virtualmente essere ascoltato da chiunque. Nonostante l'avvento di tecnologie più avanzate, il fascino della radio è rimasto intatto nel corso degli anni; piuttosto, l'evoluzione di Internet ha offerto a tutti noi la possibilità di improvvisarci deejay, utilizzando dei semplici software e trasmettendo i nostri programmi in Rete anziché via radio. Perché, allora, non approfittiamo di questi strumenti per creare la nostra radio pirata, con musica "no copyright" e informazioni libere dal controllo dei grandi media?

:: Dettagli tecnici

Il funzionamento di una radio in streaming non è molto complesso (v. Figura 1): tutto ciò di cui abbiamo bisogno è un server di streaming, che riceve un flusso di dati audio proveniente dal nostro computer e lo mette a disposizione di tutti gli ascoltatori. Questa soluzione è la più versatile e consente a chiunque di trasmettere senza avere problemi di banda. L'unico limite è dato dal fatto che bisogna disporre di un server a cui inviare i dati: per fortuna ne esistono diversi che possono essere usati gratuitamente ed è abbastanza semplice trovarne un elenco online (ad esempio, all'indirizzo http://www.radiotoolbox.com/hosts). Una soluzione un po' più complicata, ma che ci permette di essere completamente autonomi, è quella di installare un server di streaming audio sulla nostra stessa macchina: in questo modo saremo noi stessi a fare il broadcast delle nostre trasmissioni. Il limite in questo caso è quello della banda: più che sufficiente nel caso di una ADSL e pochi ascoltatori, ma scarsa nel caso di una connessione più lenta o qualora il nostro pubblico si allarghi.

:: Installiamo il software

Le tecnologie che vanno per la maggiore nel campo dello streaming audio sono due: SHOUTCast (http://www.shoutcast.com) ed Icecast (http://icecast.org). La prima è proprietaria e il relativo software è closed source, anche se viene distribuito gratuitamente; la seconda, invece, si basa su un server open source e supporta diverse applicazioni di terze parti anch'esse distribuite

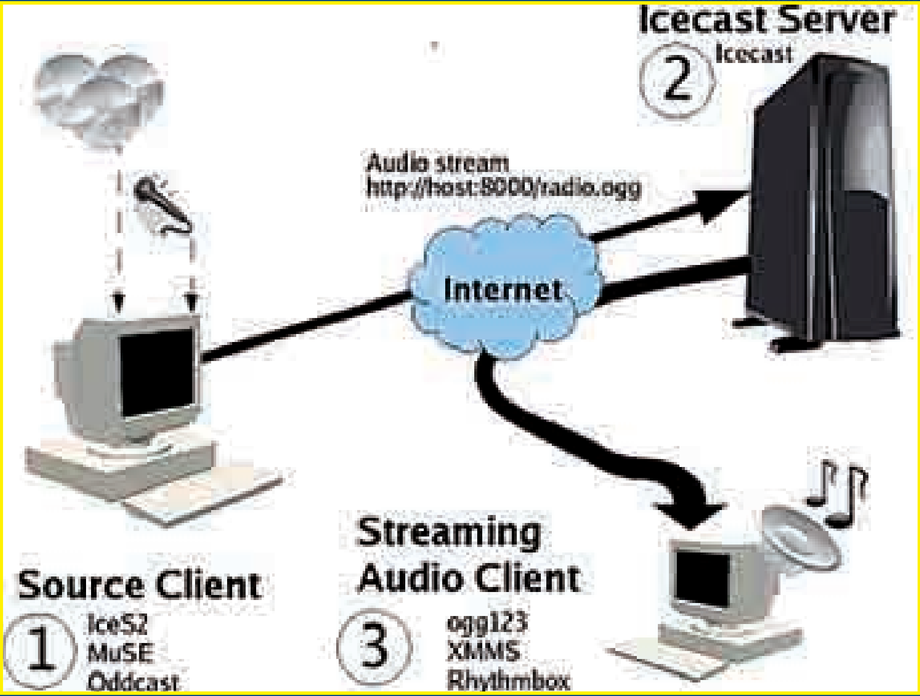
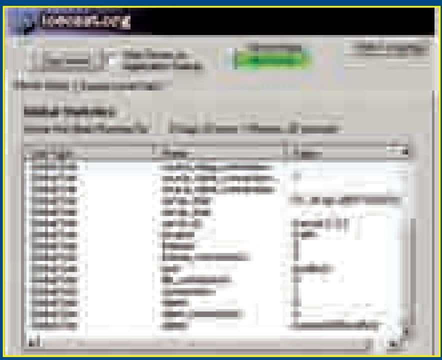


Figura 1: *I server in streaming funzionano come "ripetitori" dei segnali che noi gli inviamo, distribuendo le nostre trasmissioni a tutti gli utenti collegati.*

con licenza libera. Anche se Shoutcast è più semplice da utilizzare (il software è praticamente integrato con Winamp), la nostra scelta è caduta su Icecast in quanto decisamente più versatile. Il server Icecast è disponibile sia in versione Windows che Linux: la prima delle due ha un'interfaccia grafica mentre la seconda gira come servizio in background; ad ogni modo, in entrambi i casi la configurazione viene gestita attraverso un file di testo chiamato icecast.xml. La maggior parte delle impostazioni può essere lasciata invariata, tuttavia sarà bene sostituire la password predefinita ("hackme")

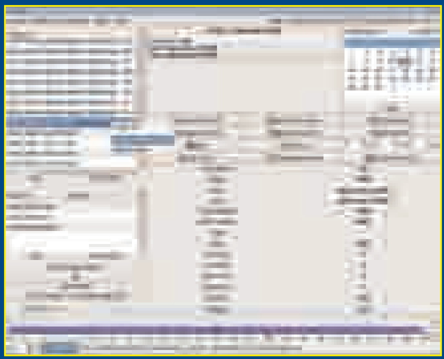


La schermata principale del server Icecast per Windows mostra le statistiche di connessione in tempo reale.

all'interno della sezione authentication. A questo punto possiamo far partire il server che si metterà in attesa di connessioni. I software che si possono collegare ad Icecast per trasmettere audio sono numerosi e diversi per genere e complessità. Fra quelli che abbiamo provato i più interessanti sono i seguenti:
LiveIce (http://star.arm.ac.uk/~spm/software/liveice.html) è un client che può essere usato come plugin per XMMS. Il suo vantaggio principale è la semplicità: è sufficiente, infatti, ascoltare dei file mp3 con XMMS per inviarli automaticamente al server Icecast;
OddCast (http://www.oddsock.org/tools/oddcastv2_wa2), l'equivalente di LiveIce per Winamp;
Muse (http://muse.dyne.org), uno strumento decisamente più evoluto, in grado di mixare fino a sei canali audio e il segnale di ingresso di una scheda audio e di salvare lo stream su disco per poterlo riutilizzare in seguito;
DyneBolic (http://dynebolic.org), infine, è una distribuzione live di Linux che offre tutti i tool necessari per creare una radio su Internet: al suo interno, naturalmente, compaiono anche IceCast e Muse.

:: Gestiamo il palinsesto

Una delle principali differenze fra una radio amatoriale e una professionale è data dalla gestione del palinsesto: i tool che abbiamo descritto finora, infatti, non sono in grado di pianificare le trasmissioni in base all'orario o riprodurre playlist come riempitivo fra diverse trasmissioni. Soma Suite (http://www.somasuite.org) è un programma in grado di supplire a queste mancanze, creando trasmissioni di diverso genere: playlist (anche generate casualmente), stream audio (nostri o presi da altre radio), file riprodotti in differita e così via.



L'interfaccia grafica di Somasuite offre una visione completa del palinsesto della nostra radio.

:: Lasciamo una traccia

Uno dei requisiti di base per una radio che si rispetti è avere degli ascoltatori. Come possiamo farci conoscere? Di sicuro, non mandando il nostro indirizzo IP (magari dinamico) in giro ogni volta che decidiamo di trasmettere. Una prima soluzione consiste nel pubblicizzare la nostra radio all'interno di un elenco: è possibile, infatti, configurare il server Icecast in modo che invii automaticamente il nostro indirizzo IP a uno di questi elenchi ogni volta che lo avviamo. Icecast stesso fornisce un elenco, ma naturalmente possiamo sceglierne altri (anche contemporaneamente). La seconda consiste nel pubblicare le nostre trasmissioni online sotto forma di podcast: in questo modo, anche chi non ha potuto sentirci in diretta avrà modo di conoscerci e di sintonizzarsi al momento giusto per ascoltare la nostra prossima trasmissione.

Hacking Printers



Con un po' di fortuna, alcune vecchie stampanti HP possono fare più di quello che sembra

Abbiamo già appreso (HJ 172) che una stampante è sì utile, ma è anche una macchina mangiasoldi: i produttori di stampanti hanno messo a punto tecniche che costringono gli utenti a usare materiali di consumo originali e, comunque, a spendere fin troppo. Si va dall'impossibilità di stampare a risoluzioni inferiori a una certa soglia per risparmiare inchiostro, all'impossibilità di riempire determinate cartucce di inchiostro e al doverle sostituire per forza dopo un certo periodo di tempo. Vediamo ora un po' più in dettaglio come funziona una stampante HP magari non recentissima ma probabilmente ancora in uso. Non si parla di un modello ben preciso, ma molte delle informazioni qui contenute possono essere compatibili con il proprio modello. Per saperlo, dobbiamo tro-

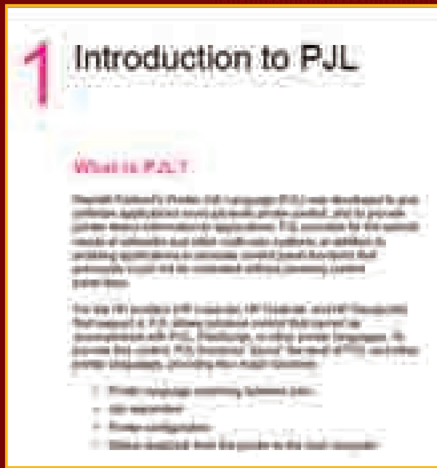


Una vecchia stampante HP Deskjet, ottimo banco di prova per allenarsi.

vare il tempo di compiere un'approfondita ricerca sul Web e scaricare qualunque tipo di documento tecnico riguardi il modello in nostro possesso.

:: I principi di base

Le stampanti, lo sappiamo, vengono pilotate dai driver installati sul computer al quale sono collegate, in locale oppure in rete. È importante però sapere che la comunicazione non è diretta dall'applicazione alla periferica: esiste un livello di astrazione tra il programma che deve stampare e l'hardware, perché è impossibile prevedere da parte dello sviluppatore come sarà configurato il sistema dell'utente. Un tempo in effetti (e si parla dei tempi del DOS) il software doveva contenere un driver specifico per poter pilotare una stampante, perché il sistema operativo non era in grado di farlo direttamente, quindi si vendevano software che comprendevano driver per le stampanti più diffuse e, viceversa, stampanti che avevano anche un disco di driver per i software più diffusi. Un vero incubo! Col tempo quindi ci si è portati sempre più verso un passaggio intermedio, traducendo il documento in un formato più o meno standard a cui il driver della stampante, ora scritto direttamente dal produttore della stessa, deve adeguarsi. E questo ci porta al primo principio alla base di questo articolo: spesso il linguaggio interno della stampante, quello che fisicamente pilota l'hardware, non ha nulla a che vedere con questo formato intermedio e normalmente non è accessibile direttamente dall'utente. Tuttavia esiste il modo di inviare comandi diretti alla stampante usando il suo linguaggio interno, in un certo modo bypassando il driver, e impostarne il funzionamento in una maniera magari non permessa dal driver stesso. Se siamo fortunati, potremmo anche trovarci tra le mani un modello di stampante del quale esiste una versione superiore, ovviamente più costosa, che differisce da questo per alcune limitazioni (per esempio, il modello economico può stampare in "bozza" ma a 600x600 dpi, mentre quello superiore può scendere fino a 300x300 dpi con notevole risparmio sull'inchiostro). Spesso infatti il modello superiore monta lo stesso identico hardware, stessa scheda interna e stesso processore, e la limitazione di quello economico è imposta dal driver di stampa.


1 Introduction to PJL

Sul sito HP si può trovare, scavando bene in profondità e in formato PDF, la manualistica tecnica sui linguaggi di stampa in formato, come il PJL.

Se siamo in grado di inviare direttamente comandi alla stampante, senza passare dal driver, potremmo essere in grado anche di superare queste limitazioni.

:: La Matrioska dei linguaggi

Le stampanti HP vengono pilotate da un annidamento di comandi in diversi linguaggi, ognuno dei quali serve per una ben determinata operazione. L'incapsulamento esterno di solito usa il linguaggio script PJL (Printer Job Language), ed è quello che gestisce il lavoro generale della stampante. In realtà, più che un linguaggio PJL è un formato di file, composto da linee di testo che contengono istruzioni in un altro linguaggio intermedio: normalmente tutte le stampanti HP comprendono perfettamente almeno uno o due dialetti dei linguaggi di codifica PCL (Printer Common Language), per esempio PCL5 o PCL6. Il linguaggio PCL è quello che effettivamente ordina alla stampante la modalità di stampa da adottare. Infine, un terzo linguaggio interno (PML, EML o altri) si occupa di pilotare direttamente l'hardware. Quest'ultimo linguaggio però non è in alcun modo accessibile da parte dell'utente, a meno che non modifichi pesantemente la stampante per scavalcarne il processore interno e ne conosca approfonditamente le specifiche, la mappa di memoria e non sappia perfettamente quello che sta facendo, pena guasti anche gravi all'hardware della periferica. Detto così, potrebbe sembrare anche semplice riuscire a pilotare direttamente la stampante per farle fare quello che vogliamo noi. In realtà le cose non stanno proprio così: malgrado la presenza di linguaggi compatibili con diversi modelli di stampante, bisogna tener presente che spesso ogni modello possiede istruzio-

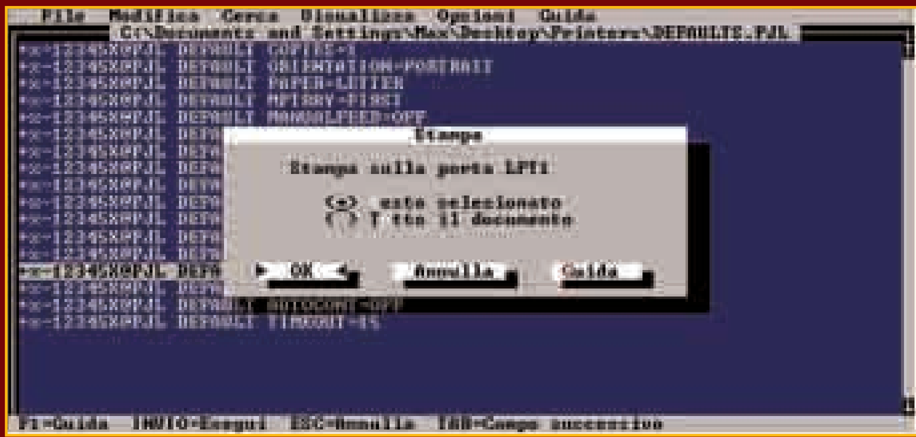
[Codice 1]

```
<esc>%-12345X@PJL DEFAULT COPIES=1
<esc>%-12345X@PJL DEFAULT ORIENTATION=PORTRAIT
<esc>%-12345X@PJL DEFAULT PAPER=LETTER
<esc>%-12345X@PJL DEFAULT MPTRAY=FIRST
<esc>%-12345X@PJL DEFAULT MANUALFEED=OFF
<esc>%-12345X@PJL DEFAULT FORMLINES=60
<esc>%-12345X@PJL DEFAULT LPARM:PCL SYMSET=PC8
<esc>%-12345X@PJL DEFAULT LPARM:PCL PITCH= 10.00
<esc>%-12345X@PJL DEFAULT LPARM:PCL FONTSOURCE=I
<esc>%-12345X@PJL DEFAULT LPARM:PCL FONTNUMBER=0
<esc>%-12345X@PJL DEFAULT ECONOMODE=OFF
<esc>%-12345X@PJL DEFAULT DENSITY=3
<esc>%-12345X@PJL DEFAULT RET=MEDIUM
<esc>%-12345X@PJL DEFAULT RESOLUTION=600
<esc>%-12345X@PJL DEFAULT PAGEPROTECT=AUTO
<esc>%-12345X@PJL DEFAULT AUTOCONT=OFF
<esc>%-12345X@PJL DEFAULT TIMEOUT=15
```

ni specifiche che non vengono divulgate da HP, se non dietro pagamento per i programmi di partnership di cui sopra. In più, esistono variazioni di questi linguaggi create appositamente per rendere alcune stampanti strettamente legate a un sistema operativo e quindi incompatibili con altri. Questo succede maggiormente per Windows che per altri sistemi.

:: Hackeriamo la stampante

Entrando in profondità nei meandri del sito HP, cercando bene tra i download e i documenti che riguardano il nostro modello di stampante o anche modelli simili, possiamo trovare un file che funge da template per le istruzioni PJL/PCL che, inviate alla stampante, ne impostano le modalità. Con un po' di fortuna, possiamo tentare di scavalcare le limitazioni del driver di stampa di Windows e impostare modalità non previste, sempre che l'hardware della periferica le supporti. In Codice 1 è riportato il file DEFAULTS.PJL distribuito da HP. Per tentare questo hack non possiamo usare Windows, altrimenti passeremo comunque per il driver della stampante, che potrebbe avere delle limitazioni. La soluzione ideale è usare un sistema MS-DOS o Linux, che pilota direttamente la porta della stampante. Un tentativo può essere effettuato dal Prompt dei comandi di Windows XP ma non è garantito che funzioni. Il carattere <esc> è il carattere Escape ed è quello che indica alla stampante che sta per ricevere un comando. Nell'editor di MS-DOS lo si può ottenere tenendo



Modifichiamo il file DEFAULTS.PJL, quindi selezioniamo e inviamo alla nostra stampante solo la linea in cui abbiamo cambiato il parametro desiderato.

premuto il tasto Alt e battendo sul tastierino numerico 27 (che è il codice ASCII proprio del carattere Escape). Se usiamo il file DEFAULTS.PJL preformato non dovremo preoccuparcene, ma se vogliamo crearne uno ex-novo dovremo tenerne conto. A questo punto possiamo tentare l'hack: forziamo la stampante a funzionare a 300 dpi anziché a 600, modificando la linea contenente il comando DEFAULT RESOLUTION=600 in DEFAULT RESOLUTION=300. Ora (ci basiamo sull'editor di MS-DOS, quindi per Linux o altri editor di testo dovremo adattare le istruzioni seguenti) stampiamo solo la linea modificata, selezionando File->Stampa e, nella finestra di dialogo mostrata, l'opzione Testo selezionato. In questo modo verrà inviato alla stampante solamente il comando modificato, lasciando invariati gli altri parametri.

Si possono verificare due situazioni. Nella migliore delle ipotesi, la stampante ha capito il comando e si è impostata di conseguenza, possiamo quindi provare a stampare qualcosa per verificarne il risultato: se ha funzionato, potremo tentare con altri parametri, per esempio cambiando il font predefinito usato per la stampa del testo. Altrimenti, può darsi che il firmware della stampante sia programmato per ignorare qualunque valore di risoluzione inferiore ai 600 dpi, o potrebbe non capire del tutto il linguaggio PJL/PCL che abbiamo usato. In questo caso, siamo davvero sfortunati e non c'è molto che possiamo fare. Se il tentativo ha avuto successo, possiamo tentare anche di forzare la stampante a usare la modalità monocromatica (bianco e nero), con il comando @PJL SET MODE=MONO o @PJL SET COLOR=MONO.

STAMPANTI E SOLDI FALSI

Circolano leggende a proposito di loschi figuri che sono stati capaci di stampare euro falsi usando scanner e comuni stampanti ad alta risoluzione (fotografiche), e li hanno usati con successo in distributori automatici di vario genere. Niente di più falso. Innanzitutto, per quanto possiamo cercare, non troveremo mai e poi mai un tipo di carta adatto, con la giusta luminosità e consistenza. Non potremo nemmeno ricreare fili metallici, filigrane e ologrammi che sono presenti nelle banconote dall'avvento dell'euro, dimentichiamocelo proprio. Ma anche se tutto questo fosse possibile, riuscire a stampare una banconota falsa e ingannare un distributore automatico rimane utopico: le stampanti usano una tecnica di stampa basata sulla quadricromia, cioè la combinazione di inchiostro di quattro colori diversi (ciano, giallo, magenta e nero), mentre i sensori ottici e gli scanner interni delle "macchinette" sono tarati per usare il sistema RGB, quindi non riusciranno mai a "leggere" una stampa in quadricromia, per cui ogni tentativo darà come risultato "soldi falsi". Inutile sperare anche nelle tolleranze introdotte di fabbrica, per consentire a questi dispositivi di accettare banconote usurate o sporche. Al massimo, se ne esistono ancora in circolazione, si può ingannare qualche distributore vecchissimo, per un pacchetto di sigarette o preservativi, ma tentare è comunque un inutile spreco di tempo. Occhio poi: oltre a essere evidentemente illegale, si rischia grosso a causa dei circuiti di videosorveglianza.



ADOBE FA ACQUA

Adobe Reader è sotto accusa: sembra che chiunque faccia un attacco tenti per prima cosa di bucare il noto lettore di PDF

Si chiama Mikko Hypponen e dalla Rsa Conference di San Francisco ha lanciato un appello che ha fatto il giro del mondo: non usate Adobe Reader! Il solito mitomane? Un tizio tutto cantina e computer? Mica tanto: Mikko Hypponen è Chief Research Officer di F-Secure. In pratica è il responsabile della sicurezza di un'azienda che fa sicurezza, il non plus ultra delle voci autorevoli in questo campo. La sua accusa è precisa e circostanziata: il 47% degli attacchi ai sistemi informativi rilevati dall'inizio dell'anno hanno avuto come protagoniste le sei falle riscontrate nell'applicazione. Sarebbe una situazione anche piuttosto tranquilla se non fosse che Adobe non ha provveduto a correggerle con particolare celerità. Piuttosto, sostiene Hypponen, se l'è presa comoda, distribuendo patch con il contagocce e con tempistiche decisamente superiori a qualsiasi altro competitor. Tempistiche talmente lunghe che l'accusatore ha persino affermato che Adobe dovrebbe prendere lezioni da Microsoft!



PDF Reader? Su pdfreaders.org!

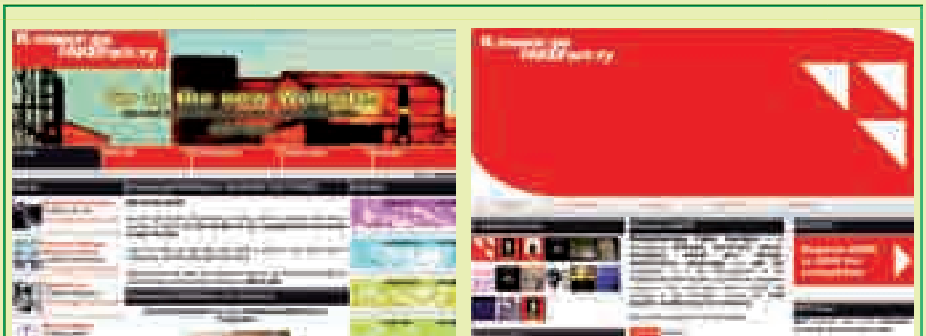
:: Pericolo!

Motivo dello scandalo è che il problema risulta piuttosto serio a causa della diffusione mondiale dei plug-in di Adobe per i vari browser e le falle sembrano essere tutt'altro che trascurabili: si va da problemi di sicurezza in senso stretto a falle che consentono la tecnica del cross site scripting (XSS) che permettono l'esecuzione di codice malevolo da remoto e l'interferenza con le funzionalità del client. Problemi che arrivano anche alla possibilità di usare i plug-in di Adobe per attacchi Denial of Service (Internet Explorer + Acrobat reader plugin, la combinazione più diffusa in assoluto) oppure il session riding (Acrobat Reader plugin con Opera, Internet Explorer oppure Firefox). Non è che pensando a plug-in diversi da Adobe reader le cose cambino molto: Hypponen stesso sembra più preoccupato da Flash e dalla possibilità di creare file swf maligni. Per questi motivi, per la prima volta, sembra che tutti gli esperti di sicurezza stiano convergendo sull'idea di Hypponen: consigliare gli utenti di usare sistemi alternativi ai plugin Adobe, rimandandoli a programmi freeware o Open Source almeno per la lettura dei file PDF. Una soluzione che ovviamente è osteggiata da Adobe che ben presto sarà costretta a correre ai ripari e iniziare a garantire una migliore assistenza per i suoi prodotti gratuiti. Come fa, appunto, Microsoft.

I pirati del RomaeuropaFAKEFactory



A gennaio scoppia in rete – forse ne avrete sentito parlare - il caso Romaeuropa WebFactory. Il concorso, promosso da Fondazione Romaeuropa e Telecom, si rivolge ai giovani creativi digitali, ma vieta per regolamento l'uso di tecniche di manipolazione come remix, mashup, imponendo la cessione gratuita e perpetua dei diritti sulle opere. Quella che vi raccontiamo è la storia del RomaeuropaFAKEFactory (REFF), la ver-



La vecchia e la nuova versione del sito. La nuova è online da aprile. Per altre informazioni, diamogli un'occhiata di persona: www.romaeuropa.org.

sione rivista e corretta da Art is Open Source, reazione critica a una politica culturale conservatrice e restrittiva per i diritti degli autori. Il progetto è supportato da circa 20 volontari e da una rete di oltre 70 partner.

:: Lo squatting del dominio

Il dominio www.romaeuropa.org inavvertitamente è lasciato libero dalla Fondazione e passano infatti poche ore fra la scoperta del caso Web Factory e il suo acquisto. I passi successivi saranno la lettera aperta “Freedom for Remix”, rivolta ai promotori di WebFactory , e la sistematica destrutturazione del concorso originario per confezionare un fake d’autore. Mutuando l’estetica del sito, il disclaimer legale e le regole di partecipazione vengono puntualmente rivoltate: remix, citazione e libertà di copyright diventano i prerequisiti del concorso, con l’aggiunta della sezione Law Art, il remix legislativo realizzato assemblando testi legali in materia di proprietà intellettuale. Mentre arrivano le prime risposte pubbliche della Fondazione Romaeuropa - “le critiche sono ampiamente condivisibili...” - a febbraio partono sito e call internazionale. Intanto su YouTube compare la serie di video “Rejected from Romaeuropa WebFactory”: i redivivi Burroughs e Wharol rifiutati dalla competizione, sviluppano una riflessione sull’arte nel contemporaneo. Conclude la serie Orson Wells, scegliendo subito la versione “fake”- un omaggio al suo celebre film del ‘75. I tre guru invocati dall’oltretomba diventano testimonial del REFF e l’èquipe si prepara al rilancio con REFF.erence, un evento che attraverserà Roma passando dalle presentazioni più istituzionali fino al clubbing notturno.

:: Gli untori

REFF.erence riesce nel suo intento: essere un momento di attraversamento, valorizzare le spinte culturali e di trasformazione che nascono dagli interstizi. Ma anche di più. La conferenza viene usata per lanciare un tavolo sulla cultura digitale in Commissione Cultura al Senato, con l’obiettivo di esplorare le relazioni fra proprietà intellettuale, nuovi modelli di business, arte e creatività: il REFF ne sarebbe lo stimolo e la cornice teorico/interpretativa. In sala è presente una delegazione della Fondazione Romaeuropa e a distanza di qualche giorno il WebFactory annuncia la modifica parziale del regolamento: gli artisti rimarranno proprietari dei diritti di sfruttamento economici delle opere, salvo iniziative culturali e di promozione legate al concorso. Negli stessi giorni il REFF entra nel calendario delle iniziative italiane dell’Anno Europeo della Creatività e dell’Innovazione. La nuova versione del sito è una piattaforma per la gestione di competizioni artistiche sviluppata con software opensource. In autunno, in programma una pubblicazione che raccoglierà gli interventi degli oltre 40 membri che partecipano al comitato scientifico e un happening performativo/espositivo distribuito fra Roma, New York e Londra. Il tutto a zero budget. Per gli autori né premi né classifiche lineari, ma un modello di promozione/valorizzazione culturale reale: le opere saranno recensite da curatori, comitato scientifico e utenti attraverso un processo aperto e visibile online. RomaeuropaFAKEFactory non è “solo” una competizione artistica. Il REFF è un’azione di hacking, dove l’attitudine del pirata tecnologico si ibrida con il situazionismo, il detournamento del linguaggio, la capacità di comunicare e di implementare quei modelli implementati dall’emersione dei media digitali. Un fake realissimo dove il “falso” diventa una felice provocazione all’esistente, superandolo.



Set fotografico “Remixing People” - REFF.jected 21 marzo, Roma – Neo Club.



William Burroughs Rejected from Romaeuropa Web Factory Prize.

penelope.di.pixel

SO DOVE SEI!



Ormai i navigatori satellitari sono in vendita ovunque con prezzi alla portata di tutti, ma le ombre di questa tecnologia possono oscurarne i vantaggi

Il 17 settembre 1959, gli Stati Uniti misero in orbita il primo dei satelliti Transit. Il suo scopo era quello di verificare sul campo la possibilità di tracciare globalmente la posizione di un oggetto a terra. Da quell'esperimento nacque un progetto che permise agli USA di tracciare con un'accuratezza non elevata ma soddisfacente la posizione di navi, aerei e sommergibili della sua flotta. Dal Transit, con l'aggiunta di satelliti e la sostituzione di quelli obsoleti, derivò quello che comunemente è chiamato GPS: Global Positioning System. Usato inizialmente solo per scopi militari, è stato reso di pubblico utilizzo nel 1991. A differenza della sua versione militare, tuttavia, in quella civile sono previste limitazioni: per impedirne l'uso sui missili stranieri, il GPS non traccia oggetti che viaggiano a più di 515 metri al secondo oppure con altezza superiore ai 18 Km. Malgrado questi limiti, tuttavia, il GPS è diventato un fenomeno commerciale sul finire del 2008, il che ha dato vita ad un abbattimento generalizzato di prezzi e ad una diffusione senza precedenti. Ormai si trovano sistemi GPS in quasi tutti i telefoni cellulari evoluti, su molte auto anche di fascia bassa o sugli scaffali del supermercato.

:: Funziona?

Il principio di funzionamento del GPS è basato, attualmente, su una costellazione di 31 satelliti in orbita attorno al pianeta, su diversi piani orbitali, disposti in modo che il ricevitore a terra possa sempre ricevere almeno 5 segnali contemporaneamente. Ciascun satellite emette segnali nella frequenza di 1, 5 GHz che vengono ricevuti facilmente a terra, in spazi aperti, da apparecchi che possono essere anche di dimensioni modeste. Il segnale emesso è composto dai parametri orbitali dell'intera costellazione di satelliti, il tempo GPS, da parametri di correzione e dall'indicazione precisa della posizione nello spazio del satellite che



La rete prevista di satelliti Galileo avrà una copertura maggiore rispetto al GPS attuale. E non sarà alla mercé degli USA.



I GPS sono diffusi nell'uso quotidiano ma anche nelle situazioni di soccorso: ogni anno permettono di salvare migliaia di vite, in mare e in montagna.

lo emette. Quest'ultima sezione, della durata di 18 secondi e ripetuta ogni 30, è l'indicazione che consente ai ricevitori, grazie al tempo GPS e ai dati dell'orbita, indicati nel segnale stesso, di calcolare, sfruttando l'effetto doppler, la corretta posizione nello spazio 3D. Sembra un'operazione molto complicata e lo è ma funziona egregiamente, con una precisione tanto maggiore quanti sono i satelliti



Tutti i cellulari dell'ultima generazione includono ricevitori GPS che permettono l'installazione di navigatori.

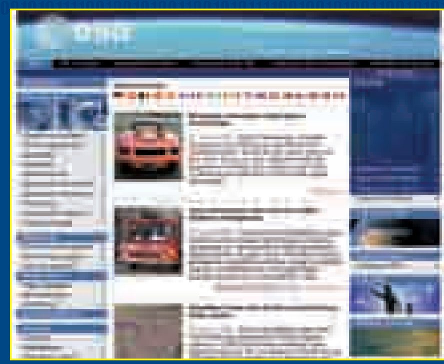
di cui si riceve il segnale. Già con 5 satelliti, in campo aperto, la precisione è di qualche metro che potrebbero scendere a pochi cm usando un maggior numero di satelliti.

:: Non ti dico dove sei!

Il condizionale è d'obbligo visto che il sistema GPS è di proprietà dell'esercito degli Stati Uniti ed è una versione meno precisa di quella effettivamente disponibile. Nello specifico, i satelliti che fanno parte della costellazione GPS emettono i segnali a 1,5 MHz usati dai ricevitori civili ma anche segnali a 1,2 MHz che si aggiungono ai precedenti quando l'uso è militare. Il vantaggio del doppio segnale è quello di annullare l'errore dovuto al fenomeno della rifrazione atmosferica, aumentando la precisione del sistema. In più, i ricevitori militari non hanno alcuna limitazione di altezza o velocità, permettendo un'applicazione illimitata. Non solo: trattandosi di un sistema proprietario di uno degli eserciti più potenti del mondo, il GPS può essere spento a piacere quando serve ai fini della nazione che lo controlla. Non è un caso che, in alcune zone del pianeta, la precisione del GPS passi di colpo da qualche metro a svariate decine oppure che sia del tutto assente una copertura del segnale. Fino ad oggi e per qualche anno ancora, quindi, le nazioni ed i privati che si affidano al GPS rischiano di mettersi alla mercé degli USA. Per queste ragioni, l'Europa ha deciso di rispondere al dominio USA con una nuova costellazione di satelliti chiamata… GPS!

:: Galileo indica la strada

Il Galileo Positioning System nasce come reazione dei paesi europei allo spadroneggiare del GPS americano e promette di superare una volta per tutte i limiti imposti alle applicazioni civili in favore di un miglioramento generale delle localizzazioni. Grazie a un piano di lanci piuttosto rigido e concordato con l'Agenzia Spaziale Europea, la sua messa in funzione ed apertura al pubblico è prevista per il 2013. Sarà compatibile e interoperabile con il GPS ma sarà più preciso,



L'agenzia spaziale europea, ESA, Ha già messo in orbita alcuni satelliti del progetto Galileo. Quando lo completerà, avremo più libertà nell'uso dei GPS.

darà una maggiore copertura, avrà un'alta disponibilità del segnale nelle aree urbane e fornirà una continuità di servizio garantita e non più dipendente dalle politiche nazionali. In più sarà molto più affidabile perché il segnale includerà messaggi di integrità del sistema, a conferma della corretta ricezione e delle condizioni generali della costellazione dei satelliti. Saranno tempi duri per l'esercito USA, abituato a muoversi da posizioni di vantaggio e, di certo, la reazione americana ci sarà. Per ora, però, si intravedono spiragli per chi ha acquistato un ricevitore GPS e si è improvvisamente ritrovato cieco, specialmente nel sud Europa, a causa di qualche azione dell'esercito USA a migliaia di Km di distanza.

TRIANGOLAZIONI

Per calcolare la sua posizione nello spazio 3D, un ricevitore stima innanzitutto la differenza tra il suo orologio interno e quella di un segnale ricevuto da un satellite e si sincronizza. Poi calcola il ritardo di propagazione del segnale tra l'indicazione arrivata con il segnale stesso e il suo orologio. In questo modo, moltiplicando il ritardo per la velocità della luce, ottiene la sua distanza effettiva dal satellite. Questa distanza può essere vista come una sfera attorno al satellite che ha inviato il segnale. Ripetendo questa operazione per diversi satelliti, il ricevitore riesce a calcolare il punto di intersezione di tutte le sfere, pari alla sua posizione reale nello spazio.

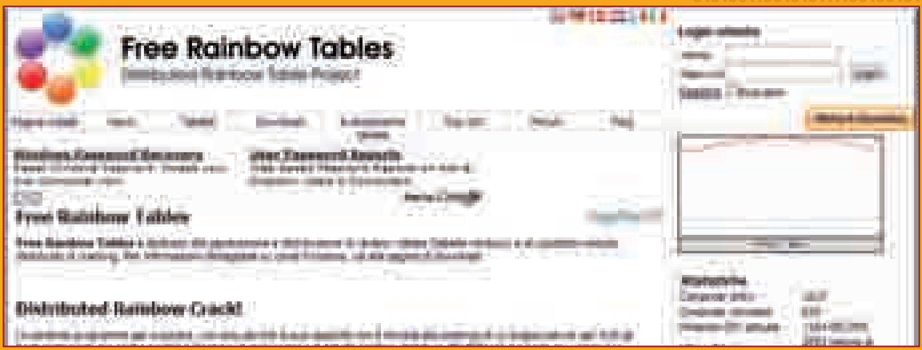
Il brute force è superato da un pezzo: per craccare una password è ormai indispensabile ricorrere a metodi ben più furbi

Un arcobaleno di password

Andare per tentativi nel recupero di una password, anche usando script e programmi dedicati, è quanto meno problematico a causa del tempo necessario anche per craccare password semplici. Noto anche come ricerca esaustiva, il brute force porta sempre a trovare la password cercata ma ha il difetto di richiedere tempi piuttosto lunghi: ogni possibile password viene provata alla ricerca di quella corretta. La ricerca si può rendere più veloce svolgendo un processo in parallelo, magari tramite software di calcolo distribuito, ma molti problemi sono decisamente difficili da affrontare con questo metodo. Un approccio migliore si basa sull'uso di dizionari. Partendo dal presupposto che le password usate sono generalmente mnemoniche, specialmente per gli accessi degli utenti, è lecito pensare che, prima di provare qualsiasi combinazione di caratteri, si utilizzino le parole della lingua dell'utente o di altre lingue del pianeta. Per questo motivo, oggi, si tende a passare dal concetto di password a quello di passphrase: non una singola parola ma un'intera frase che un utente può ricordare facilmente ma che risulta decisamente complessa da identificare per tutti gli altri.

:: L'hash

Un approccio diverso, più tecnico e mirato è quello che coinvolge l'uso delle rainbow tables: tabelle costruite in modo particolare e capaci di diminuire notevolmente i tempi di forcing delle password. Frutto di un lavoro teorico sviluppato da Martin Hellman nel 1980, le rainbow tables sono la dimostrazione di come l'uso di tabelle precompilate renda decisamente più veloce la ricerca di chiavi. In linea di principio si tratta di un approccio che potrebbe effettivamente diminuire in modo drastico i tempi di ricerca ma la sua applicazione pratica è affidata alla corretta compilazione delle tabelle stesse ed è ostacolata da un problema di natura pratica: una compilazione completa di hash richiederebbe diversi Terabyte di spazio, con evidenti problemi di storage. Una soluzione a questo problema è stata trova-



Sul sito www.freerainbowtables.com c'è un'intera community che si sta occupando di generare rainbow tables usando un sistema di calcolo distribuito.

ta dall'esperto di sicurezza Philippe Oechslin che creò tabelle che hanno come righe le rainbow tables in cui sono memorizzate solo la password iniziale e quella finale e come colonne degli hash. Ogni tabella viene poi creata usando catene che vanno da un determinato hash a un altro, a cui si applicano funzioni di riduzione diverse per ogni colonna. Punto fermo di tutta la teoria è che ogni tabella viene costruita usando un'unica funzione di hash, così da semplificare sia il lavoro di ricerca che di costruzione. La funzione di riduzione, variabile, viene invece usata per generare una password partendo da un hash determinato. L'algoritmo di ricerca prevede che data una password iniziale, ne venga generato un hash a cui viene applicata l'ultima funzione di riduzione della catena. Il risultato viene poi confrontato con l'ultimo hash di ogni catena in tabella. Se corrisponde viene ricostruita la catena corrispondente. Se l'hash non compare, partendo dalla riga inferiore verrà applicata la funzione di riduzione e verranno riapplicate sia la funzione di hash che quella di riduzione facendo il dovuto confronto con la posizione in tabella, fino a ricadere nel caso in cui l'hash viene trovato oppure fino a quando non si esaurisce la tabella.

:: In pratica...

Il procedimento appare piuttosto complesso e lo è ma è anche il sistema attualmente più utilizzato per il crack delle password. Anche se la generazione delle rainbow tables è al di là della portata di moltissimi computer, Internet ci mette a disposizione diversi siti da cui scaricare tabelle utili. Allo stesso tempo, pur con un algoritmo complesso, il sistema è veramente efficace: il tempo necessario per superare password complesse è mediamente di un settimo rispetto ad altri sistemi e la possibilità di trovare la password corretta sfiora il 100%. Praticamente è quasi come un brute force ma con la differenza che il tempo di ricerca necessario, a parità di condizioni di elaborazione, è drasticamente ridotto. L'unico metodo possibile per contrastare questo genere di crack è quello di aumentare artificiosamente la lunghezza e la complessità delle password, ricorrendo a una tecnica chiamata salt: l'aggiunta di bit casuali a una password in modo da modificarne artificiosamente l'hash. Sapendo quali sono i bit aggiunti e avendo l'hash finale, un sistema può sapere se la password inserita è corretta pur registrando un hash diverso da quello che ci si aspetterebbe.

:: Provo anche io!

Attualmente, il software più diffuso che utilizza le rainbow tables è il celebre John The Ripper: un software sviluppato per sistemi operativi UNIX e attualmente eseguibile per diverse piattaforme. La sua caratteristica principale è quella di combinare tra loro diverse tecniche di crack delle password e un'estrema flessibilità d'utilizzo. Nativamente, può decifrare password DES, MD5 e Blowfish ma dispone di estensioni che gli permettono non solo di affrontare la decrittazione tramite rainbow tables ma anche i sistemi MD4 usati comunemente da LDAP e MySQL. Si scarica dal sito www.openwall.com/john e una sua prova sul campo è vivamente consigliata. Per chi desidera un approccio orientato esclusivamente alle rainbow tables è consigliabile una prova di Ophcrack. Open Source, si scarica dal sito ophcrack.sourceforge.net e dispone anche di un LiveCD che ne permette l'uso senza installazione.



Ophcrack è un programma utile per comprendere il sistema con cui vengono usate le rainbow tables. Uno sguardo al suo sorgente è illuminante più di mille spiegazioni.



John The Ripper è un programma di crack delle password che, con un plugin, può utilizzare le rainbow tables: un vantaggio in più per penetrare nei sistemi.



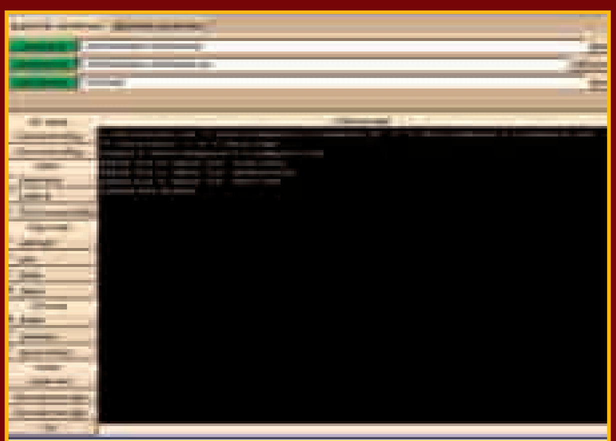
TUTTO SOTTO CONTROLLO

Preveniamo le intrusioni nella nostra rete con Snort

Non è semplice, anche se in realtà serve solamente un po' di attenzione e di pazienza, ma preparare un computer per tenere sotto controllo il traffico di rete ed essere avvisati nel caso di anomalie è alla portata di tutti ed è gratuito. Ci vuole pazienza perché si devono installare diversi software, sistemare alcuni file di configurazione e ci vuole del tempo per decomprimere archivi particolarmente pesanti, come quello delle regole per Snort e relativi messaggi di log.

:: La sistemazione ideale

Dato che per disporre di un sistema efficace Snort deve girare sempre, è meglio usare un computer ad hoc, magari quello vecchio di cui non sappiamo bene che fare. Potrebbe andare bene anche un Pentium III, ma come al solito maggiore è la potenza e più veloci saranno le operazioni. Meglio poi partire da un'installazione di Windows XP almeno con SP2 pulita, cioè solo il sistema operativo e null'altro. Dobbiamo quindi procurarci tutto il software necessario: sul sito http://www.snort.org è a disposizione una comoda guida passo-passo per l'installazione che comprende l'elenco dei programmi, ma per comodità la riportiamo anche in Tabella 1. Seguendo attentamente le indicazioni riportate sulla guida di installazione per Windows XP (http://www.snort.org/docs/setup_guides/Snort%20Windows%20XP%20Guide.txt), non si dovrebbero incontrare problemi particolari. È solo un processo laborioso che in situazioni particolari, come un PC non troppo potente, potrebbe richiedere diverso tempo. Al termine avremo una macchina dedicata esclusivamente all'analisi del traffico di rete, in grado di riportarci immediatamente ogni anomalia. Ma a cosa ci serve?



L'interfaccia grafica utile per gestire le regole di Snort mediante Oinkmaster: non dobbiamo quindi spostare a mano migliaia di file nelle cartelle giuste.

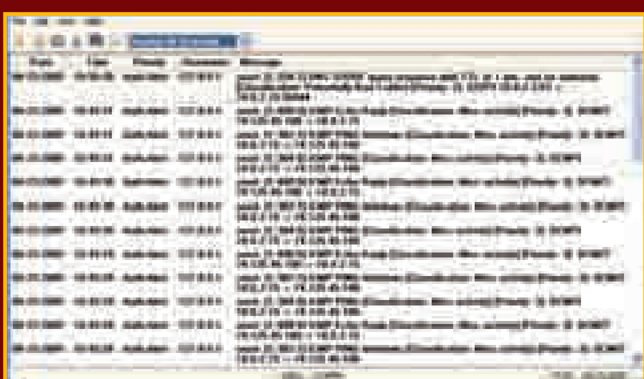
SOFTWARE	INDIRIZZO WEB
Microsoft Windows XP + SP2	http://www.microsoft.it
Mozilla Firefox	http://www.mozilla-europe.org/it/firefox/
AVG Antivirus Free Edition	http://free.avg.com/download?prd=afe
Zone Alarm Free Firewall	http://www.zonealarm.com/security/it/zonealarm-pc-security-free-firewall.htm
Microsoft Baseline Security Analyzer	http://www.microsoft.com/downloads/details.aspx?FamilyId=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en
ActivePerl	http://www.activestate.com/store/productdetail.aspx?prdGuid=81fbce82-6bd5-49bc-a915-08d58c2648ca
Notepad++	http://sourceforge.net/project/showfiles.php?group_id=95717&package_id=102072
Foxit Reader	http://www.foxitsoftware.com/pdf/reader/download.php
Kiwi Syslog Server	http://www.kiwisyslog.com/kiwi-syslog-server-overview/
7-Zip	http://www.7-zip.org/
WinPCap	http://www.winpcap.org/install/default.htm
Snort	http://www.snort.org/dl/binaries/win32/
Oinkmaster (con GUI)	http://oinkmaster.sourceforge.net/download.shtml

:: L'analisi del traffico

Innanzitutto, vediamo come funziona il sistema che abbiamo appena preparato. Si tratta in sostanza di un packet analyzer, che cattura i pacchetti in transito sulla rete (compito di WinPCap) e li analizza secondo determinate regole (Snort + Oinkmaster) per presentarci un log adeguatamente formattato e di facile lettura (Kiwi Syslog Server) quando individua un'anomalia. Dato che ogni attacco portato verso una rete informatica è riconoscibile da determinate firme lasciate dal comportamento del cracker, come pacchetti spurii o appositamente malformati, è relativamente facile con un software come Snort accorgersi di cosa sta succedendo quasi in tempo reale, e prendere le adeguate contromisure. In più, questo ci permette di individuare più facilmente eventuali falle di sicurezza dei nostri sistemi, con la possibilità di porvi rimedio prima che qualche malintenzionato se ne accorga e ne approfitti.

:: Le regole

Per decidere se un determinato schema di pacchetti corrisponde a un tentativo di attacco, Snort utilizza delle regole, cioè dei file di testo che riportano pattern da ritenere sospetti. Dato che si tratta di molti file, è impensabile gestirle manualmente e quindi se ne occupa Oinkmaster. È uno script perl che si occupa di scaricare quasi automaticamente eventuali aggiornamenti delle regole disponibili sul sito di Snort e di installarli nel nostro sistema. Il tutto avviene per mezzo di una comoda interfaccia grafica. I file delle regole contengono semplicemente informazioni di testo, usate dal programma per un confronto con i pacchetti catturati. Non vanno in alcun modo modificati se non sappiamo esattamente cosa stiamo facendo: sono approntati da un team di esperti di sicurezza appositamente per il funzionamento di Snort. Eventualmente, in fase di configurazione, possiamo decidere di includere o no determinati insiemi di regole (escludendo quelle inutili: niente regole P2P se non usiamo tali programmi) . All'inizio però è meglio includerle tutte, almeno ai fini dell'apprendimento. Col tempo, poi, potremo escludere pian piano quelle che non ci servono.



Kiwi intercetta ogni segnalazione di Snort e la visualizza in modo chiaro e facilmente leggibile per permetterci di analizzarla con calma e prendere le adeguate contromisure.

:: Mettiamolo alla prova

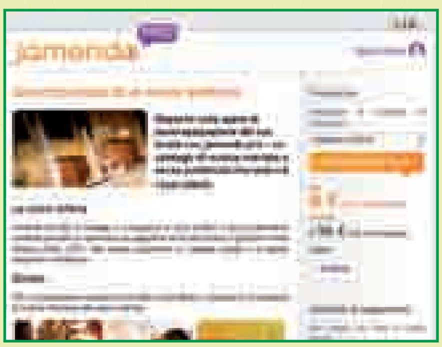
Vediamo all'atto pratico come funziona il nostro sistema antintrusione. Innanzitutto, scarichiamo eventuali aggiornamenti delle regole: se abbiamo seguito le istruzioni, troviamo sul desktop il file perl Update Snort Rules. Lanciamolo per avviare l'interfaccia di Oinkmaster, facciamo clic su Update Rules! e attendiamo che l'aggiornamento termini (nella finestra del programma troveremo la scritta "done.") prima di procedere. Lanciamo il file SnortStart.bat, sempre creato in fase di configurazione. Attendiamo qualche minuto fino al completo caricamento di Snort (vedremo il maialino stilizzato) e avviamo quindi Kiwi Syslog Server. Ora tutto è pronto per verificare sul campo ciò che il sistema è in grado di segnalarci. Apriamo una finestra del Prompt dei comandi e lanciamo un ping verso un qualunque dominio. Mentre nella finestra del prompt scorrono le risposte del server, in quella di Kiwi appaiono le segnalazioni dei pacchetti di risposta. Dato che alcuni attacchi usano proprio questi pacchetti, Snort li segnala diligentemente e il log di queste segnalazioni viene ripreso e visualizzato da Kiwi. Se troviamo nel log messaggi non provocati da nostre azioni, dovremmo preoccuparci e verificare attentamente che cosa sta succedendo sulla nostra rete, perché è molto probabile che qualcuno stia tentando di infilarsi.



La SIAE non la pago

Nel lettore Mp3, nel CD, nell'hard disk appena arrivato, nella radio, in TV, sul Web, al bar... Invasori alieni? No, è la SIAE

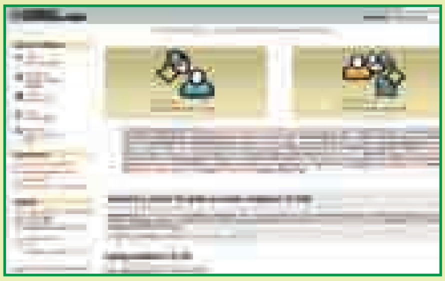
Cos'hanno in comune un appassionato di tecnologia che cambia hard disk, il proprietario del bar sotto casa, la nonna che guarda la TV, un papà che riprende la sua bimba, l'appassionato che compra un MP3 online e il ragazzino che acquista il CD del suo idolo? A prima vista sono persone che vivono in mondi diversi, ma un fattore comune ce l'hanno: è la Società Italiana Autori ed Editori, meglio nota come SIAE. Tutti pagano o concorrono al pagamento dei diritti che spettano alla SIAE ovunque ci siano, praticamente o potenzialmente, audio o video tutelati dai diritti d'autore. Speranza vana, quella di poter elencare le cose per cui è necessario pagare la SIAE: trasmissioni televisive, uso di brani musicali tutelati, duplicazione di CD e DVD, diffusioni sonore di radio e così via. Ma la SIAE si paga anche per cose meno scontate: con la scusa che si possono usare strumenti vari per fare copie di materiale tutelato, la SIAE incamera abbondanti profitti in percentuale sul prezzo di vendita di unità dati. Non solo lettori MP3 ma anche schede di memoria, nastri per backup, hard disk, CD, DVD, cellulari e chi più ne ha, più ne metta. Ma non solo… La SIAE si incamera diritti per riproduzioni in pubblico di materiale presso bar, ristoranti, sale d'attesa, stadi, teatri, manifestazioni di beneficenza, feste scolastiche e altro ancora. In alcuni casi, come per i bar, i pagamenti vanno avanti secondo criteri quanto meno discutibili: al di là delle dimensioni del locale, conta la fisicità. Con un impianto che legge i CD e 2 casse si ha un prezzo. Con un impianto radio se ne ha un altro. Aumentando il numero di casse, aumenta il balzello...



Il servizio di contributi per la diffusione pubblica di Jamendo, pro.jamendo.com, costa meno della SIAE e offre ottima qualità audio. Può essere una valida alternativa.

:: Adesso la freghiamo

Attenzione, però: la SIAE può essere molto tentacolare ma non ha più una valenza assoluta. Se, fino a qualche anno fa, la SIAE controllava tutta la musica, tutti i video, tutte le opere di qualsiasi genere, oggi le cose stanno cambiando a favore di un approccio più "open". Questo cambiamento nasce dal fatto che ci sono in circolazione migliaia e migliaia di opere che sono state create da persone che non sono iscritte alla SIAE. Di più: ci sono



Creative Commons Italia sta cercando un'intesa con SIAE per la tutela dei diritti e delle libertà individuali. Sarà difficile comunque arrivare ad un accordo.

migliaia di opere la cui licenza di utilizzo è esplicitamente gratuita oppure che sono diffuse con piattaforme che prevedono il pagamento ad altri enti di tutela. Un esempio che si sta affermando anche in Italia è quello di Jamendo, pro.jamendo.com. Si paga un abbonamento annuale calcolato sulla base delle dimensioni del locale e lo staff di Jamendo fornisce una chiavetta USB, un lettore MP4 o 30 CD con la sua musica selezionata, comprensiva dei diritti di diffusione in pubblico. Certo, non ci si deve aspettare di poter trasmettere le ultime hit, ma il catalogo Jamendo si distingue grazie a una cura qualitativa almeno pari a quella delle migliori radio. A variare, moltissimo, è il prezzo: per un locale di 100 metri quadri, con qualsiasi numero di diffusori, il costo annuale è inferiore a 100 euro. Ovviamente, la SIAE non sta a guardare: è impossibile decidere di usare questo sistema e pensare di esser lasciati in pace dagli ispettori. Per evitare i continui controlli e le multe, che vengono elevate perché "non si sa mai", purtroppo, occorre sottostare alla solita burocrazia e chiedere alla SIAE stessa di aprire una procedura speciale facendo presente che tutta la propria programmazione musicale è tutelata da un altro ente. Procedura lunga ma che vale la pena: perché pagare inutilmente i diritti d'utilizzo di qualcosa che in realtà non si usa effettivamente?



Report si è occupata tempo fa della SIAE con un'inchiesta illuminante da cui è risultato che Report stessa non è tutelata dalla SIAE. Ma Costanzo sì.

SEI COSE CHE NON QUADRANO

Da anni, ormai, la SIAE è accusata in modo diretto o strisciante di essere un organismo che ha trasformato la sua opera di tutela in un sistema vessatorio nei confronti dei cittadini e delle aziende. In particolare sono sei i punti controversi per cui la SIAE è periodicamente messa sul banco degli imputati.

- **Equo compenso**
La SIAE percepisce una percentuale sul prezzo di vendita dei supporti vergini venduti in Italia (CD, DVD, Videocassette, memorie digitali, hard disk, pellicole fotografiche...) presumendo che siano destinate ad ospitare materiale protetto, in barba all'utilizzo normale fatto con questi supporti: fotografie proprie, dati di PC, opere non tutelate, eccetera.
- **Compensi per eventi non lucrativi**
Ovviamente, la SIAE non fa sconti per nessuno. Tantomeno quando chiede compensi per manifestazioni senza scopo di lucro oppure per manifestazioni di sostegno a iniziative sociali. Incluse le recite dei bambini dell'asilo e i concerti di beneficenza.
- **Compensi per usi didattici**
Diversamente da quanto accade per altre società di tutela, all'estero, la SIAE non ammette il concetto di fair use. I diritti si pagano anche quando le opere vengono usate a scopo di studio o didattico: da un professore che vuole mostrare un quadro, da un maestro che vuole far ascoltare un concerto agli allievi e via dicendo.
- **Ha un potere legislativo**
La SIAE svolge un ruolo di primo piano nel comitato consultivo per il diritto d'autore, che emana norme a cui la stessa SIAE deve attenersi.
- **Ha un monopolio legale sull'attività di intermediazione**
Diversamente da altri paesi, la SIAE ha la concessione di stato per qualsiasi attività di intermediazione tra utenti e produttori e opera in un mercato assolutamente chiuso. Qualsiasi atto di concorrenza avviene per concessione della SIAE stessa.
- **Coniuga copyright e diritto d'autore**
Questa confusione impedisce agli autori di poter condividere le proprie opere anche senza scopo di lucro. Un autore che organizzasse un concerto gratuito, di opere scritte in proprio, in cui lui fosse l'unico esecutore, sarebbe comunque costretto a pagare i diritti alla SIAE.

::Il primo passo

Il movimento contro queste gabelle medioevali, adatte ad un contesto sociale degli Anni '70 e ormai superate dalla contaminazione internazionale delle opere, tipica della nostra società 2.0, è appena nato e i successi sono ancora pochi.
Proprio a causa del suo essere così tentacolare, la SIAE incamera ogni anno diversi milioni di euro, distribuiti con metodi che lasciano perplessi anche ad alcuni autori ma i soldi fanno gola a molti. Non è lontano, però, il giorno in cui, finalmente, la legge permetterà in modo più semplice un libero mercato dei diritti d'autore e la SIAE si renderà conto che la sua posizione di predominio non deriva da una effettiva condizione di favore di mercato per i suoi iscritti ma dalla pura, brutale, imposizione di leggi ormai vetuste. In attesa di quel momento, possiamo comunque goderci, personalmente, le possibilità offerte dalle radio internazionali, dalle fonti libere e dagli autori che hanno scelto forme di diffusione delle loro opere al di fuori dei canali tradizionali. Per la libera diffusione dobbiamo piegarci alle procedure SIAE ma è solo una questione di tempo...

Symantec ha presentato il suo ISTR: l'annuale rapporto sulle tendenze degli attacchi ai sistemi informativi

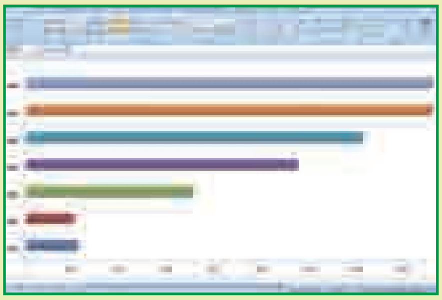


Borsino attacchi

Spam in crescita, virus in crescita, phishing in crescita... Gli attacchi alla sicurezza sembrano non conoscere alcuna crisi. Per questo motivo, l'uscita dell'Internet Security Threat Report di Symantec è stata attensa con ansia: è l'appuntamento annuale che permette agli esperti di sicurezza di fare il punto della situazione e cercare di prevedere le contromisure che sarà necessario prendere durante l'anno per garantirsi una infrastruttura IT pulita. La possibilità di dare uno sguardo a un report prodotto grazie alle diverse sonde di cui Symantec dispone nel mondo, dai client antivirus dei normali utenti ai sistemi di intercettazione nelle Web Farm, è senz'altro un'occasione d'oro per gli addetti ai lavori. L'attesa è stata ancora più spasmodica pensando al caso Conflicker, virus purtroppo ben noto la cui diffusione è stata senza precedenti a causa delle innovative tecniche di infezione utilizzate.

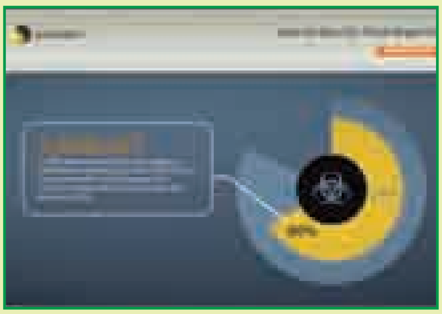
:: Dramma

Il rapporto, è doveroso dirlo, non è affatto buono, anzi. Il quadro che ne esce è piuttosto sconsolante, specialmente per il nostro Paese. A fronte di un sistema IT mondiale che soffre della crisi, di aziende che vanno al risparmio su tutto, trascurando spesso la sicurezza, l'Italia si distingue per una scalata in classifiche in cui vincono gli ultimi. Guadagniamo un posto nella classifica delle attività malevole registrate, ben due posti in quella dei paesi originari degli attacchi, un posto tra i paesi con più computer infetti da bot. Insomma: stiamo andando alla conquista di un podio che sarebbe meglio lasciare ad altri. A consolarci, se si può dire, c'è il fatto che il resto del mondo non ha fatto grandissimi progressi. Con l'esclusione



Il numero di attacchi globali nel 2008 è decisamente più alto che negli anni scorsi ma non come la crescita del numero di utenti avrebbe fatto prevedere.

di pochi paesi che sono riusciti a contenere gli attacchi grazie alla lungimiranza di utenti ed amministratori, il resto del pianeta si batte costantemente contro la crescita di quasi tutti i reati informatici, problema di cui soffrono in modo marcato, manco a dirlo, i paesi che stanno investendo sulla banda larga. Come se non bastasse è quanto meno imbarazzante che al primo posto come Stato canaglia di Internet, titolo attribuito al Paese che più di tutti ospita gli attaccanti, ci siano proprio gli Stati Uniti. Alla faccia di chi vuole pensare che gli attaccanti siano sempre est europei o di qualche sperduto paese esotico. Con meno della metà delle origini di attacco, al secondo posto, troviamo la Cina, seguita dall'Ucraina.



Il report è liberamente consultabile all'indirizzo eval.symantec.com/flashdemos/threat_report_xiv/

::Obiettivo comune

Punto focale di quasi tutti gli attacchi, in qualsiasi ambito, a qualsiasi livello e da qualunque parte provengano, è la conquista dei dati personali. Dati delle carte di credito, certo, ma anche password di accesso a siti e servizi Web, furti di identità, dati di login dell'home banking. Gli attacchi mirati alla conquista di informazioni riservate assommano a ben il 76% del totale e hanno caratteristiche decisamente variegate: dal phishing sugli utenti al cracking delle password dei sistemi, dalla SQL Injection nei siti Web all'installazione di keylogger. Una nota tutta speciale riguarda la trasformazione sempre più frequente di malware in prodotti del tutto simili a quelli commerciali, offerti gratuitamente agli utenti: da un'analisi dei trend del "mercato" sembra che questa moda esploderà nell'anno in corso, con tragiche conseguenze su milioni di account.

:: Tutto male, tutto bene

Anche se la lettura di questo report è scoraggiante, però, occorre anche considerare un problema di contesto in cui sono stati rilevati i dati. Ogni informazione è stata ricavata da sonde e ridotta a un dato puro ma, si sa, le statistiche bisogna leggerle attentamente per capirle. Così possiamo tranquillamente affermare che la situazione, specialmente quella italiana, non è così peggiorata. O meglio: potrebbe essere



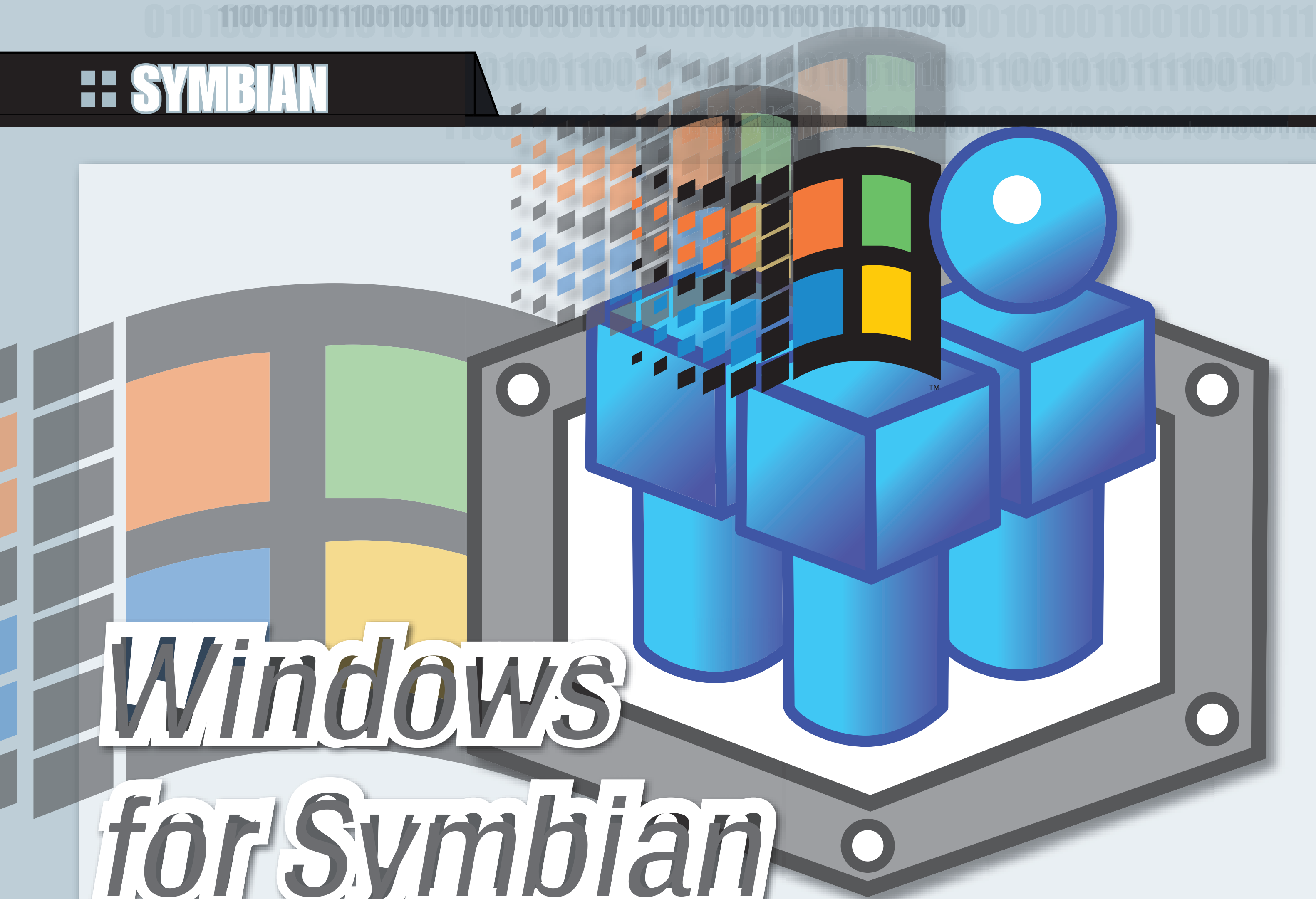
Symantec dispone di un lab che monitorizza l'intero network di client ed è una vera autorità nel campo. Finora ha identificato oltre 2,6 milioni di minacce.

ben peggiore. Il motivo alla base di un giudizio più leggero sta nel fatto che la popolazione di Internet nel mondo è tutt'altro che costante. Nel nostro paese il numero di abbonati nel 2008 alla banda larga è aumentato a dismisura, l'alfabetizzazione media informatica non si è mossa minimamente e, per questo, è già un bene che gli attacchi non siano esplosi in maniera più devastante. Lo stesso avviene in altre parti del mondo, in cui il livello di crescita numerica degli utenti non ha una corrispondenza con la crescita dell'alfabetizzazione nel campo IT. Complessivamente, quindi, se una lettura iniziale può scoraggiare, un'analisi secondo questa chiave rende drasticamente meno drammatica la situazione.

SEMPRE PIU' PERICOLOSO

Il numero di attacchi aumenta costantemente di anno in anno. Oltre a un aumento globale dell'alfabetizzazione informatica, che aumenta il numero di bersagli e di attaccanti, sono 7 le cause che fanno da volano a questa tendenza.

1) I download dai siti Web sono in costante crescita.
2) Gli attacchi sono sempre più spesso offuscati e basati su un codice in trasformazione, rendendo spesso inefficaci gli antivirus.
3) Il maggior numero di attacchi non viene più diretto verso i browser ma verso i plugin, generalmente l'anello più debole della catena.
4) Gli utenti installano sempre più spesso applicazioni di dubbia provenienza, portatrici di virus.
5) Gli attacchi SQL Injection sono diretti spesso verso i maggiori siti Web.
6) Il mercato vede un aumento di pubblicità che dirigono gli utenti verso siti di dubbia funzionalità.
7) Vi è una vera e propria esplosione di esempi di codice per creare malware disponibili a chiunque.



Windows for Symbian

Vediamo come rivivere i vecchi tempi sul nostro smartphone

Avevamo anticipato qualche numero fa la possibilità di far girare Windows sui recenti modelli di smartphone con Symbian 3a versione. In questo articolo descriviamo come riuscirci. Cosa ci occorre:

- un telefonino con Symbian 3a versione e almeno 128Mb di ram;
- una scheda di memoria esterna abbastanza capiente (512Mb+);
- DOS-BOX compilato per Symbian;
- ovviamente i file di installazione di Windows.

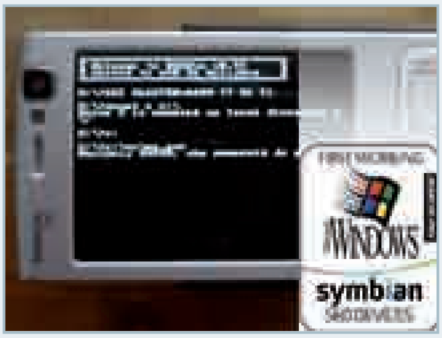
:: Setup di DOS-BOX

Tramite un motore di ricerca è possibile trovare il pacchetto "tutto incluso" realizzato da un programmatore polacco che ha scelto come nickname Marcin-prv. Per prima cosa ha realizzato il porting verso Symbian di DOSBox v0.72 (www.dosbox.com), un emulatore x86 del DOS ed è riuscito ad installare Windows 3.1. Nel caso foste più audaci potreste sempre provare a scaricare i sorgenti open-source di DOSBox e cross-compilarli su Linux o Windows per processori ARM e creare gli archivi .sis (tramite Nokia SDK ad esempio) come ha fatto lui. Reperito l'archivio, conviene decomprimerlo sul PC. Nella cartella di DOSBox troveremo due versioni di file .sis relative a installazioni che occupano più o meno memoria. Proviamo prima a installare la versione full (DOSBox_Full.sisx). In caso di errore per mancanza di memoria, ricorriamo alla versione slim (DOSBox_Slim.sisx). Vanno poi installati tutti i pacchetti .sis e .sisx presenti nella cartella install (glib.SIS, pips_nokia_1_3_SS.sis, RGA.sis, SDL-1.2.13-s60-2.3.4_armv5.sisx, ssl.SIS, stdcpp.SIS, stdioserver_s60_1_3_SS.SIS) dopodiché DOSBox potrà essere lanciato per verificarne il corretto funzionamento. Conviene quindi copiare la cartella sulla memoria esterna e lanciare gli installer, uno alla volta, direttamente dal telefonino. Se tutto si installa correttamente, DOSBox è pronto e possiamo verificare che parta: lanciandolo vedremo il familiare prompt del dos apparire dopo una man-



Installare il sisx di DOSBox non è sufficiente, vanno installati anche tutti i pacchetti contenuti nella cartella install.

ciata di secondi. Ricordiamoci che per passare dalla modalità di inserimento al prompt del DOS basta cliccare sul tasto verde di chiamata.



DOSBox emula anche una scheda audio Sound Blaster compatibile e diverse unità di massa (floppy, hard disk, CD-ROM).

:: Windows 3.1

Premettendo che andrebbe installata solo una versione legalmente acquistata (ammesso che si possieda ancora la licenza!), scompattiamo l'archivio Win3.1-on-s60v3_v1.0_(Marcin-prv).rar direttamente nella memoria esterna del telefonino nella cartella e:\data\win31 e verifichiamo che nel file e:\data\dosbox.conf compaiano le seguenti righe:

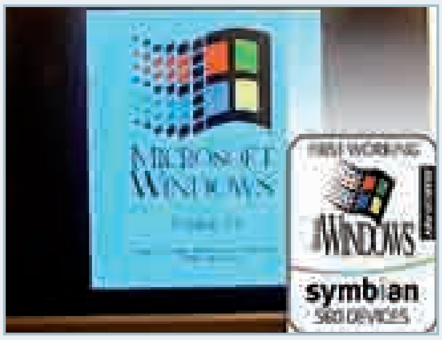
mount c e:\Data
mount d e:
c:
c:\Windows\win.com

Lanciando ora DOSBox verrà dapprima caricato l'emulatore del dos e successivamente Windows 3.1, in cui è stato aggiunto Calmira II: un modding scritto in Delphi 1.0 che rende l'interfaccia molto simile a Windows 95 e ne riprende alcune funzionalità come Taskbar, Start menu, System Tray e altro.



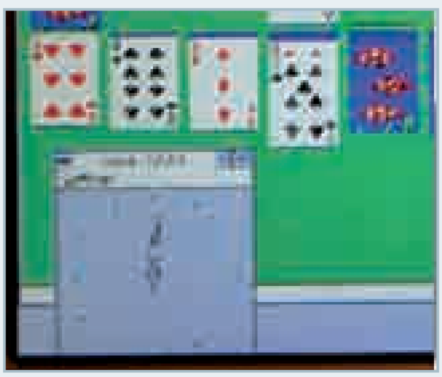
Nello stesso archivio di Windows 3.1 c'è anche lo storico Norton Commander che è possibile far partire sostituendo c:\Windows\win.com con c:\nc\nc.exe in dosbox.conf.

Il boot sul telefonino usato per le prove (un E51) è abbastanza rapido ma la resa sul piccolo schermo non è così soddisfacente. Con un terminale con matrice più grande, l'usabilità e la leggibilità migliorano sensibilmente: Marcin-prv ha utilizzato un N95. Per poter usare le frecce per spostare il mouse va premuto una volta il tasto verde di chiamata (permette di switchare tra modalità mouse e modalità tastiera), mentre il tasto di selezione permette di emulare il clic del mouse.



La versione classica di Windows 3.1 parte in pochissimi secondi facendo dimenticare le lunghe attese che si avevano sui primi x86!

Se ci fossero problemi di RAM, in dosbox.conf è possibile aumentare il parametro memsize, di default impostato 2.



La versione dell'orologio e del solitario di Windows 3.1 su DOS-BOX.

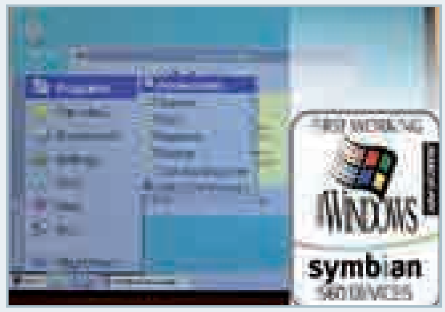
:: Windows 95/98

Se abbiamo sufficiente RAM (e potenza di calcolo) nel telefonino possiamo provare anche Windows 95 e addirittura Windows 98!

Sempre nel pacchetto di Marcin-prv sono infatti presenti anche le immagini di questi sistemi operativi e versioni di dosbox.conf già configurato. È sufficiente decomprimere l'immagine w95.img o w98.img in e:\dos\Windows\ e modificare in dosbox.conf le righe in [autoexec] in questo modo (sostituendo w9x.img con l'immagine scelta):

[autoexec]
Lines in this section will be run at startup.
imgmount c e:\dos\Windows\w9x.img -t hdd -fs fat
boot -l c

Purtroppo, sul telefonino usato per le prove già Windows 95 sembra troppo pesante per essere gestito. Per provare Windows 98 consigliamo quindi avere un N82/N95 o superiore.



Con Calmira II Windows 3.1 sembra proprio Windows 95, ma resta la leggerezza che avevamo dimenticato.

:: Sviluppi futuri

Sembra che qualcuno stia già tentando di realizzare immagini di Windows XP che, se funzionasse, equivarrebbe a dire di avere in piccolo la potenza di calcolo di un recente desktop, con tutte le possibilità che ne conseguono.Tuttavia già l'esperienza con Windows 9x permette di provare una certa emozione, nonostante il sistema operativo non sia stato studiato per un'interfaccia spartana come quella del telefonino. Va da sé che siamo nell'ambito del retro-computing e del puro esperimento, ma a differenza di altri casi il tutto avviene nel palmo della nostra mano e l'effetto è davvero notevole.

Massimiliano Brasile